JL

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 May 2003 (01.05.2003)

PCT

(10) International Publication Number
WO 03/036845 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US02/33286

(22) International Filing Date: 18 October 2002 (18.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/037,593 19 October 2001 (19.10.2001) US

(71) Applicant *(for all designated States except US)*: **GLOBAL VELOCITY, L.L.C.** [US/US]; 211 N. Broadway, Suite 2200, St. Louis, MO 63102 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KULIG, Matthew, P.** [—/—]; 19 Danube Dr., Millstadt, IL 62260 (US). **BROOKS, Timmy, L.** [—/—]; 1836 Meadow Trails Dr., St. Louis, MO 63130 (US). **LOCKWOOD, John, W.** [—/—]; 839 Jackson Ave., St. Louis, MO 63130 (US). **REDDICK, David, Kyle** [—/—]; 512 S. Clay Ave., Kirkwood, MO 63122 (US).

(74) Agents: **BERTANI, Mary Jo** et al.; Koestner Bertani LLP, 18662 MacArthur Blvd., Suite 400, Irvine, CA 92612 (US).

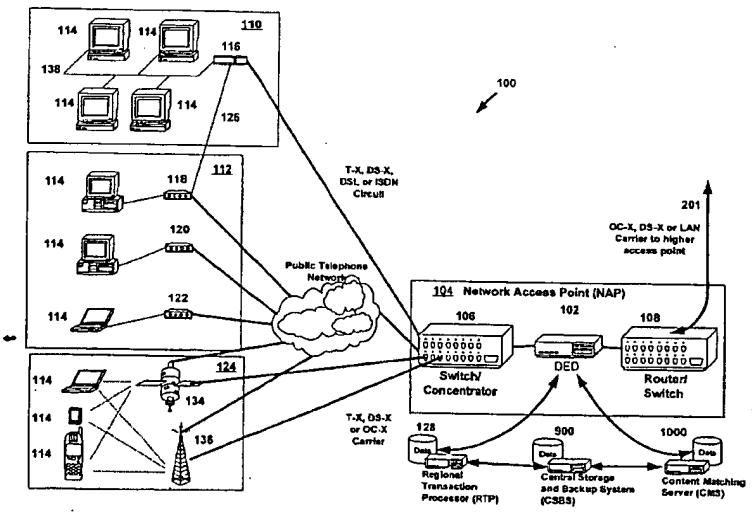
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR CONTROLLING TRANSMISSION OF DATA PACKETS OVER AN INFORMATION NETWORK



(57) Abstract: An apparatus for controlling transmission of data packets in an information network comprises a Regional Transaction Processor (RTP) operable to communicate with a Data Enabling Device (DED) and at least one workstation. The DED searches data packets for content match information. The RTP includes instructions to generate information to include in a prompt to be presented at the workstation when the content match information is detected in at least one of the data packets. The prompt is based on information in the data packet. Transmission of the data packets through the information network is suspended by the DED until a response to the prompt is received that authorizes downloading the data packets to the workstation. If transmission of the data packets to the workstation is not authorized, the data packets are discarded by the DED.

WO 03/036845 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

System And Method For Controlling Transmission of Data Packets Over An Information Network

BACKGROUND OF THE INVENTION

Description of the Related Art

Information can be transmitted faster and more easily than ever since the advent of the computerized information networks, such as the Internet. Facsimile machines, computers, and electronic appliances such as personal digital assistants (PDAs) and wireless telephones with Internet access enable the quick transfer of information to remote locations around the world.

The capability to quickly and easily transfer information does, however, have certain drawbacks. Information in digital form, while readily transferable, may also be accessed by more entities than ever before, including those who are not intended to be recipients. Copyrighted digital content can often be illegally sent from point A to point B without being detected, files can be corrupted or infected with viruses that can shut down recipients' computers, and confidential information can be transmitted or posted on publicly accessible network sites. For these reasons, electronic content providers, businesses, and individual users are increasingly concerned with copyright protection, virus protection, and security issues.

Commercial content providers are concerned with the prevalent copying without compensation of digital content, such as compact disks (CDs), electronic books, digital movies, and digital video disks (DVDs). Individual content users often are at cross purposes with content providers, desiring unauthorized copying of content, including digital music, software programs, movies, digital books, images and the like. Content creators, who desire as wide an audience as possible, often are torn between dissemination goals and compensation goals.

The Internet Backbone provides the major interconnections between disparate networks and includes the following components:

Network service providers (NSP) which operate the networks that route packets of data from point to point. A NSP offers National/International interconnecting Internet services to internet service providers (ISPs) through network access points (NAPs).

Long Distance Carriers (telephone) provide a national network of communication channels for the Internet as well as other long distance voice and data communication needs. In general, the NAP contracts with a Long Distance Carrier for the channels needed for their backbone.

Network Access Points (NAPs) provide for the exchange of packets between networks operated by the Network Service Providers.

Primary National Service Providers collectively operate what is often referred to as the Public Internet Backbone. Each Primary National Service Provider operates one or more Wide Area Networks, typically using either Frame Relay and/or asynchronous transfer mode (ATM) architectures on a national basis. Local ISPs typically use these Primary National Service Providers as their interface point to the Internet Backbone.

Primary National Service Providers and National Internet Service Providers exchange packets at Network Access Points. The routers used by a backbone provider use Border Gateway Protocol (BGP) to dynamically learn routes. When the owner of an IP address changes ISP providers, it announces its new provider to the rest of the world using BGP, which causes the world's routers to adjust their routing tables to account for the change.

Point of Purchase (POP) locations of digital content currently reside within the workstation networks of digital content suppliers and Internet retailers. Network Access Points (NAPs), such as network service providers, currently do not have the ability to control or charge for the re-transmittal of digital content.

Outside of digital content workstations or supplier systems, Federal, State and local governments currently do not have the ability to identify potentially taxable transactions, such as the transmission of digital content for sale between a content

provider and a user, or retail purchases. Similarly, there currently are no systems to impose, track, and protect taxation of identified digital content on a state, or local level for point-to-point transfers between non-authorized suppliers of digital content.

There currently are numerous methods used to identify and protect digital content between suppliers and users, but each method has limitations.

One method of protecting information uses watermark technology, which marks rendered works, including text, digital pictures, and digital audio with information that identifies the work or the publisher. The human eye can read some types of watermarks, while other types can be read only electronically.

Another known security technique uses fingerprint technology. The term fingerprint is sometimes used in contrast with watermarks to form a message digest of the document. Fingerprinting is typically accomplished using one of a number of types of hash functions. A common hash function is the one-way hash function that provides a fixed-length hash value, h, after operating on an arbitrary-length pre-image message. The h is unique to the message associated with it. However, the security of the h depends on the number of bits of the hash. A practical size is 128. There are a number of different types of hashing algorithms, including the Message Digest (MD) 4 algorithm, and the MD5 algorithm, which is more complex than the MD4 algorithm. Another type of hash function is the n-hash algorithm, which implements a random function hashing and logical exclusive OR functions.

Another aspect of the security of electronic content pertains to Digital Rights Management (DRM). DRM entails establishing and managing rights and permissions for digital content and supports distribution of digital content. DRM can be used for digital distribution of educational, professional and trade content as well as entertainment content. However, DRM imposes new hardware and software requirements on users to facilitate its implementation, and does not easily integrate with existing systems in the marketplace.

Another method of protecting information involves the use of cryptographic key solutions. One type of cryptographic key solution uses symmetric keys in which

an encryption key can be calculated from the decryption key and vice versa. A more secure key solution uses asymmetric keys in which the key used for encryption is different from the key used for decryption. A user desiring to communicate with another retrieves the destination certificate from a database and verifies authenticity. Verifying authenticity often involves several Certification Authorities (CAs) if there is a hierarchy of CAs between the user's CA and the destination CA. After verification, communication may take place by using the keys to "unlock" encrypted containers containing the protected messages. Typically, timestamps are used to confirm that messages are current. Alternatively, a three-way protocol involves the user checking a random number that was originally generated by the user, sent to the destination, and received back from the destination. Likewise, the destination checks a random number received from the user that was originally generated at the destination. This type of security is not conducive to mass distribution of digital content.

Another alternative for limiting unauthorized access involves monitoring network traffic at the internal network level through firewalls, proxy servers, or access lists. These systems are designed to prevent users from accessing pre-designated sites or pre-designated file types over the Internet. This approach applies access rules to prevent files having designated attributes, such as particular suffix, from being transferred into and/or out of the organization. The access rules can be cumbersome and costly to establish and maintain for both small and large organizations.

Another form of security relates to virus protection. Virus protection is a global issue with the advent of the Internet and impacts large and small organizations and individual users. Virus scanning is currently performed at end local nodes and workstations. Thus, viruses can be stopped only once they have spread and been identified within these systems. This approach cannot prevent viruses from spreading prior to being distributed to the local nodes or workstations.

U.S. Patent No. 5,629,980 describes a system which provides for the secure and accounted-for distribution of digitally encoded works. The owner of a digital work attaches rights to the work that define how that work may be used and further

distributed. It is assumed that digital works reside on a secure depository, and depart only when the requestor meets certain rights. Once a digital work leaves the digital domain, e.g. it is printed out, played or otherwise rendered, it is no longer secure and can be copied by unauthorized users.

U.S. Patent No. 6,233,684 describes a system for controlling the distribution and use of rendered digital works though watermarking. It is assumed that there are trusted entities on the Internet that enforce certain rules for watermarks and fingerprints whenever content is duplicated. First, a social reminder appears on the material to indicate whether duplication is acceptable. Second, auditing features record when copies are made. Third, copy detection is enforced so that duplicates can be differentiated from originals.

U.S. Patent No. 6,112,181 describes systems and methods for matching, selecting, narrowcasting, and/or classifying content based on rights management and/or other information. A matching and classification system is used to filter masses of data for the benefit of the user. The system proposes a "matchmaker" to locate content, which would have value to the user, but ignores content that would be irrelevant. Thus, this tool focuses on helping a user identify content he or she may want to purchase. It does not assist the provider with a means to bill the user.

U.S. Patent No. 6,233,618 describes a technique to limit access to information content available on the Internet. The technique includes filtering data and is implemented within a network device such as a proxy server, router, switch, firewall, bridge or other network gateway. Information about the site to which the request for data was made is used to help determine whether or not the material should be filtered. The access control process analyzes data in each request from the clients and determines if the request should be forwarded for processing by a server to which it is destined.

U.S. Patent No. 6,216,173 discloses a system in which the content of a packet determines its routing through a network. The path a packet follows through the network is determined, at least partially, by the type of data carried within the packet

itself. For example, a web request could be fulfilled by routing a packet to a nearby router. Some requests can be processed by software on the local workstation.

U.S. Patent No. 6,205,148 describes selecting a higher-level protocol for packets in a router. Usually, routers enumerate each of the possible protocols for packets, then send that number as a field in the packet. This is done, for example, with IP packets. Each IP packet determines if the embedded packet uses, for example, the TCP or UDP protocols. The disclosure deals primarily with asynchronous transfer mode (ATM), and means to identify packets that could be transmitted over ATM.

The currently known methods, such as the methods described in the preceding paragraphs, are designed for denying access to designated data or sites, rather than allowing free flow of digital content over the Internet. Currently known methods do not provide capability for conducting transactions on designated digital content at a price established by authorized selling agents and content owners, or a standard tool for blocking designated digital content from unauthorized users. A transaction gateway point is needed that provides better data management both going to and coming from the Internet backbone than what is provided by currently known systems. Once this gateway point is established, applications can be installed that solve many data management issues.

SUMMARY

A system and method in accordance with an embodiment of the present invention provides a transaction gateway point with a data enabling point at the NAPs to non-intrusively manage data packets transmitted on the Internet backbone is provided.

In one embodiment, a system for controlling transmission of data packets in an information network in accordance with an embodiment of the present invention comprises a Regional Transaction Processor (RTP) operable to communicate with a Data Enabling Device (DED) and at least one workstation. The DED searches data packets for content match information. The RTP includes instructions to generate

information to include in a prompt to be presented at the workstation when the content match information is detected in at least one of the data packets. The prompt is based on information in the at least one data packet. Transmission of the data packets through the information network is suspended by the DED until a response to the prompt is received that authorizes downloading the data packets to the workstation. If transmission of the data packets to the workstation is not authorized, the data packets are discarded by the DED.

In one aspect of this embodiment, the prompt is based on the content match information.

In another aspect of this embodiment, the DED is operable to detect when the one or more data packets include content match information at a rate proportional to the rate at which the data packets are received.

In another aspect of this embodiment, the DED prevents further transmission of the one or more data packets based on the content match information.

In another aspect of this embodiment, the RTP comprises a network server and a database, and is operable to process transactions for requests for content.

In another aspect of this embodiment, the DED is located at a Network Access Point (NAP).

In another aspect of this embodiment, the system includes a plurality of DEDs along a network route. Each DED is operable to communicate with at least one of the other DEDs. The plurality of DEDs include a first DED that generates the prompt and one or more intermediate DEDs operable to forward the prompt to the DED closest to the workstation along the network route. The plurality of DEDs are operable to communicate with each other to prevent transmitting more than one prompt for the same data packet through the network route.

In another aspect of this embodiment, the RTP transmits a Release_Content or Cease_Content message to the DED, based on whether the at least one data packet was authorized to be downloaded to the workstation.

In another aspect of this embodiment, the DED includes field programmable gate arrays (FPGAs). The FPGAs can be reprogrammed over the network to perform a content matching function in accordance with an embodiment of the present invention.

In another aspect of this embodiment, a portion of the DED can be dynamically reprogrammed and the DED is operable to continue processing the data packets during the partial reprogramming.

In another aspect of this embodiment, the DED includes a hardware-based data packet processor and a software-based data packet processor.

In another aspect of this embodiment, a CSBS communicates with the RTP to monitor operation of the RTP, and to store transaction information. The CSBS is operable to transmit information to reprogram the DED to communicate with another RTP.

In another aspect of this embodiment, a content matching server (CMS) is operable to store content match information, to communicate with the DED, and to transmit the content match information to the DED.

In another aspect of this embodiment, the DED is operable to suspend transmission of the data packets through the information network until a response to the prompt is received.

In another embodiment, a method for controlling transmission of identifiable content over an information network in accordance with an embodiment of the present invention includes:

providing content match information for the content to a DED. The DED is located in the information network along a transmission path of a plurality of data packets. At least one data packet includes the content match information;

receiving the at least one data packet in the DED;

detecting the content match information in the at least one data packet in the DED, and

issuing a prompt to a workstation based on the content match information when the content match information is detected in the at least one data packet.

In one aspect of this embodiment, the method includes processing a transaction based on a user's response to the prompt.

In another aspect of this embodiment, the method includes transmitting a message among a plurality of DEDs along the transmission path to prevent transmitting more than one prompt for the same data packet.

In another aspect of this embodiment, the method includes processing a transaction based on the content match information, and transmitting a Release_Content or Cease_Content message to the DED based on whether content was authorized to be downloaded to the workstation during the transaction.

In another aspect of this embodiment, the method includes reprogramming a portion of the DED to detect different content match information.

In another aspect of this embodiment, the method includes suspending transmission of the at least one data packet through the information network until a response to the prompt is received.

In another embodiment, an apparatus for controlling transmission of data packets in an information network includes a Regional Transaction Processor (RTP) operable to communicate with a DED and at least one workstation. The DED detects content match information in at least one of the data packets. The RTP includes instructions to generate information to include in a prompt to be presented at the workstation. The prompt is based on information in the at least one data packet.

In one aspect of this embodiment, the DED detects the content match information at a rate proportional to the rate at which the data packets are received.

In another aspect of this embodiment, the DED prevents further transmission of one or more of the data packets based on the information in the at least one data packet.

In another aspect of this embodiment, the RTP further comprises instructions to process a transaction based on the information in the at least one data packet.

In another aspect of this embodiment, a plurality of DEDs are positioned along a network route, and each DED communicates with at least one of the other DEDs. The plurality of DEDs include a first DED that generates a message and one or more intermediate DEDs operable to forward the message to the DED closest to the workstation along the network route. The plurality of DEDs to communicate with each other to prevent transmitting more than one message for the same data packet through the network route.

In another aspect of this embodiment, the RTP transmits a Release_Content or Cease_Content message to the DED, based on whether the at least one data packet was authorized to be downloaded to the workstation during the transaction.

In another aspect of this embodiment, a portion of the DED can be dynamically reprogrammed and the DED can continue performing content matching functions during the partial reprogramming.

In another aspect of this embodiment, the RTP communicates with a Central Storage And Backup System (CSBS). The CSBS monitors operation of the RTP, and stores transaction information.

In another aspect of this embodiment, the CSBS transmits information to reprogram the DED to communicate with another RTP.

In another aspect of this embodiment, the RTP communicates with a content matching server. The content matching server stores content match information, communicates with the DED, and transmits the content match information to the DED.

In another aspect of this embodiment, the DED suspends transmission of the at least one data packet through the information network until a response to the prompt is received.

In another embodiment, an apparatus includes a Central Storage and Backup System (CSBS) that communicates with a plurality of Regional Transaction Processors (RTPs) and provide backup storage for the RTPs. The RTPs communicate with a Data Enabling Device (DED) and at least one workstation. The DED detects content match information in at least one data packet. The RTP comprises instructions to generate information to include in a prompt to be presented at the workstation. The prompt is based on information in the data packet.

In one aspect of this embodiment, the CSBS monitors the operation of the RTPs.

In another aspect of this embodiment, the CSBS stores transaction information for the RTPs.

In another aspect of this embodiment, the CSBS maintains the content match information.

In another embodiment, a computer program product includes instructions to enable communication between a workstation, a Data Enabling Device (DED), and a Regional Transaction Processor (RTP). The DED detects content match information in at least one data packet and prevents further transmission of one or more data packets based on the information in the at least one data packet. The RTP generates information to include in a prompt to be presented at the workstation. The prompt is based on information in the at least one data packet.

The foregoing is a summary and thus contains, by necessity, simplifications, generalizations and omissions of detail; consequently, those skilled in the art will appreciate that the summary is illustrative only and is not intended to be in any way limiting. As will also be apparent to one of skill in the art, the operations disclosed herein may be implemented in a number of ways, and such changes and modifications may be made without departing from this invention and its broader aspects. Other aspects, inventive features, and advantages of the present invention, as defined solely by the claims, will become apparent in the non-limiting detailed description set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features and advantages made apparent to those skilled in the art by referencing the accompanying drawings. The use of the same reference number throughout the several figures designates a like or similar element.

Figure 1a is a diagram of a network that includes a DED at a Network Access Point (NAP) and a Regional Transaction Processor (RTP) in accordance with an embodiment of the present invention.

Figure 1b is a diagram of an example of a Regional Transaction Processor (RTP) of Fig. 1a which interacts with the DED.

Figure 1c is a diagram of an example of a Content Matching Server (CMS) of Fig. 1a which can reprogram the DED as required.

Figure 1d is a diagram of an example of a Central Storage and Backup Systems (CSBS) for storing back-up information for the RTP's shown in Fig. 1a.

Figure 1e is a flowchart of an example of a process for handling purchasing transactions using the network in Fig. 1a.

Figure 1f is a flowchart of an example of a process using the network in Fig. 1a to calculate sales tax on a transaction conducted over the network in Fig. 1a.

Figure 1g is a block diagram of an example of a workstation that is suitable for use in the network of Fig. 1a.

Figure 2a is a diagram of the International Standards Organization (ISO) Open Systems Interconnect (OSI) model showing layered data encapsulation.

Figure 2b is a diagram of layered data encapsulation.

Figure 3a is a diagram of a packetized elementary stream packet for an MPEG file.

Figure 3b is a diagram of a transport stream for an MPEG file.

Figure 4a is a flow diagram of one embodiment of a data enabling procedure that can be utilized in the network shown in Fig. 1a.

Figure 4b is a sample screen prompt presented to a private workstation when attempting to download copyright protected files with a transaction option in accordance with the process in Fig. 4a.

Figure 4c is a sample screen prompt presented to a public workstation when attempting to download copyright protected files with a transaction option in accordance with the process in Fig. 4a.

Figure 4d is a sample screen prompt presented to a workstation when attempting to download copyright protected files with no transaction option in accordance with the process in Fig. 4a.

Figure 4e is a sample screen prompt presented to a workstation when a virus is detected at the NAP and prevented from being downloaded to the workstation in accordance with the process in Fig. 4a.

Figure 4f is a sample screen prompt presented to a workstation when a virus is detected in data sent from the user at the NAP in accordance with the process in Fig. 4a.

Figure 4g is a sample screen prompt presented to a workstation when confidential data is detected at the NAP in accordance with the process in Fig. 4a.

Figure 4h is a sample screen prompt presented to a System Administrators workstation when one of the workstations on the network is attempting to transmit confidential data over the network in accordance with the process in Fig. 4a.

Figure 4i is a sample screen prompt presented to a workstation when a purchase is made over the network in accordance with the process in Fig. 4a.

Figure 5a is a block diagram of a network that includes DEDs at various levels of the network in accordance with an embodiment of the present invention.

Figure 5b is a block diagram of a network of NAPs that includes DEDs at various levels of the network in accordance with an embodiment of the present invention.

Figure 5c is a block diagram showing lines of communication between a series of DEDs along a path for transmitting data packets over the network shown in Fig. 1a.

Figure 5d is a block diagram of a series of DEDs along a path for transmitting two or more data packets associated with the same content over the network shown in Fig. 1a.

Figure 5e is a block diagram of multiplexed data packets transmitted along two unique paths in the network shown in Fig. 1a.

Figure 5f is a diagram of a network with multiple DEDs for monitoring data packets in accordance with an embodiment of the present invention.

Figure 6a is a diagram of one type of device that can be utilized as a DED that can be utilized in the network of Fig. 1a.

Figure 6b is a diagram showing a switching circuit that can forward traffic to the DED shown in Fig. 6a.

Figure 7 is a diagram of network access points and workstations that communicate with the Regional Transaction Processor (RTP) on a regional and local level in accordance with an embodiment of the present invention.

Figure 8a is a flow chart of one embodiment of a communication process between the DED, the RTP, and the workstation that can be utilized in the network shown in Fig. 1a.

Figure 8b is a flow chart of one embodiment of an initialization process to establish communication between the DED, the RTP, and the workstation that can be utilized in the network shown in Fig. 1a.

Figure 8c is a flow chart of one embodiment of a process for preventing confidential content from being transmitted onto a network from a workstation that can be utilized in the network shown in Fig. 1a.

Figure 8d is a flow chart of one embodiment of a process for preventing content infected with a virus from being transmitted over a network to a workstation that can be utilized in the network shown in Fig. 1a.

Figure 8e is a flow chart of one embodiment of a process for preventing content infected with a virus from being transmitted onto a network from a workstation that can be utilized in the network shown in Fig. 1a.

Figure 9 is a block diagram of an embodiment of a centralized data storage facility for the RTPs that can also reallocate the DEDs to different RTPs in the network shown in Fig. 1a.

Figure 10 is a block diagram of one embodiment of a Content Matching Server (CMS) for providing the DEDs shown in the network of Fig. 1a with content matching information.

Figure 11 is a block diagram of one embodiment of a point of purchase system within the NAP shown in the network of Fig. 1a.

DETAILED DESCRIPTION

Fig 1a shows an embodiment of a network 100 that includes a Data Enabling Device (DED) 102 at a Network Access Point (NAP) 104. The DED 102 can be positioned between a switch 106 and routers/switches 108. Switch 106 allows workstations 114 connected to networks 110, 112, 124 to communicate with NAP 104, and routers/switches 108 allow NAP 104 to communicate with other NAPs (not shown).

Content match information is used to identify content in a data packet and is stored in a Content Matching Server (CMS) 1000. The CMS 1000 provides copies of the content matching information to DEDs 102 to perform content matches on data packets that are transmitted to the DEDs 102. The content match information

can comprise any data string that uniquely identifies the content. For example, the content match information can be a string of digital data from the digital recording of a song. CMS 1000 can also test the uniqueness of content match information to help insure that two or more different entities are not supplying identical content match information.

The term "content match" as used herein refers to the process of comparing the content match information in the DED 102 to content match information in a data packet. For example, the DED 102 detects a content match when a string of digital data in a packet matches an identical string of data that was provided as content match information in the DED 102.

Control information is used to determine whether a data packet in which content match information was found can be transmitted to the workstation 114. The control information can include information such as an identifier for a virus, whether the content is subject to copyright protection or security (confidentiality) controls, purchase price, and/or the number of copies a user can make of the content. The control information is typically provided by the entity that wants to monitor and/or control dissemination of content, such a music recordings or books, over the network 100.

The content match information can be updated as required in the CMS 1000, which in turn updates the DED 102 with the new content match information. DED 102 non-intrusively searches data packets for the content match information. The term "non-intrusive" denotes searching the data packets for the content match information without delaying delivery of packets that do not include the content match information and are not associated with a data packet that includes content match information. When the DED 102 detects the content match information in a packet, the DED 102 invokes a Regional Transactional Processor (RTP) 128 to perform one or more transactions based on the control information. Transmission of other data packets associated with the packet containing content match information can be delayed until the transaction(s) are completed and transmission of the associated data packets is authorized.

Users access the information network 100 through a NAP, such as NAP 104. DED 102 can monitor all digital content transmitted between users connected to NAP 104 and other NAPs (not shown). Communication protocols are used to transport information from NAP to another. The protocols form a stack of layers, each layer communicating with the one above it or below it by passing information in a suitable form to the next layer.

Figure 1b shows an embodiment of a Regional Transaction Processor (RTP) 128 that includes various hardware and software components that allow RTP 128 to communicate with the DED 102, facilitate and process transactions, and store the related information securely within network 100. The router 152 routes data packets between web server 148 and DED 102 via firewall 146. Enterprise switch 144 then routes data packets to storage system 142, database (DB) server 130, accounting server 140, or remote access server 150, depending on the instructions in the control information received in the data packet.

Fig. 1c shows an embodiment of the CMS 1000 of Fig. 1a that can update the DEDs 102 as required with content match information. The remote access server 170 can receive content match information directly from content owners via communication lines connected to the content owners' servers, as well as other authorized servers. The DB server 168 and storage system 166 store the content match information. Enterprise switch 164 transmits the content match information to the DED 102 through firewall 162 and router 160. Firewall 162 includes facilities to help prevent unauthorized access to the content match information on DB server 168 and storage system 166

Fig. 1d shows an embodiment of the Central Storage and Backup System (CSBS) 900 of Fig. 1a that backs up and stores data from the RTPs 128. CSBS 900 receives data from the RTPs 128 through router 172, firewall 174, and enterprise switch 176 to back-up onto storage systems 178 and 180. DB server 182 date stamps and logs all information received. Data can also be retrieved from CSBS 900 by RTPs 128.

Fig. 1e shows an embodiment of the RTP 128 of Fig. 1a that processes transactions based on user response via from the workstation 114 and messages from the DED 102. The accounting server 140 receives and processes transactions using data in the DB server 130, the remote access server 150, and external billing systems 154, 156 to facilitate transactions.

Fig. 1f shows an embodiment of the RTP 128 of Fig. 1a having access to a tax lookup table 158 stored on the DB server 130 and/or the storage system 142. The tax table 158 can be accessed via DED 102 to determine the amount of sales tax to add to the price of delivering content or other retail transactions made by a user at the workstation 114. An identifier for the workstation 114 and an identifier for the corresponding DED 102 indicating the jurisdiction of the workstation 114 can be used to determine which tax tables or tax rate formula to use to determine the amount of federal, state and/or local sales tax to charge for a transaction. For mobile workstations 114, information can also be provided to prevent imposing local sales tax on users when they are outside their resident jurisdiction.

The various embodiments of components shown in Figs. 1b-1f can be configured in many different ways to support transactions at workstation 114, with the embodiments shown being just some examples of suitable configurations.

The DED 102 and the RTP 128 also can use public/private key encryption/decryption technology to decrypt encrypted data packets for content matching, and then re-encrypt the data packet and forward it to the workstation 114. Alternatively, content match information can be provided to identify the content of a data packet in encrypted format, thereby eliminating the need to decrypt the data packet.

Fig. 1g is a block diagram of an example of a computer system suitable for implementing the workstation 114, which includes a bus 1122 to interconnect subsystems of workstation 114 such as a central processor 1124, a system memory 1126 (typically RAM, but which may also include ROM, flash RAM, or the like), an input/output controller 1128, an external audio device such as a speaker system 1130 via an audio output interface 1132, an external device such as a display screen 1134

via display adapter 1136, serial ports 1138 and 1140, a keyboard 1142 (interfaced with a keyboard controller 1143), a storage interface 1144, a floppy disk drive 1146 operative to receive a floppy disk 1148, and an optical disc drive 1150 operative to receive an optical disc 1152. Also included are a mouse 1156 (or other point-and-click device, coupled to bus 1122 via serial port 1138), a modem 1157 (coupled to bus 1122 via serial port 1138) and a network interface 1158 (coupled directly to bus 1122).

Bus 1122 allows data communication between central processor 1124 and system memory 1126, which may include both Read Only Memory (ROM) or flash memory (neither shown), and Random Access Memory (RAM) (not shown), as previously noted. The RAM is generally the main memory into which the operating system and application programs are loaded and typically affords at least 16 megabytes of memory space. The ROM or flash memory may contain, among other code, the Basic Input-Output System (BIOS) which controls basic hardware operation such as the interaction with peripheral components. Applications resident with workstation 114 are generally stored on and accessed via a computer readable medium, such as a hard disk drive (e.g., fixed disk 1154), an optical drive (e.g., CD-ROM drive 1150), floppy disk unit 1146 or other storage medium. Additionally, applications may be in the form of electronic signals modulated in accordance with the application and data communication technology when accessed via network modem 1157 or network interface 1158.

Storage interface 1144, as with the other storage interfaces of workstation 114, may connect to a standard computer readable medium for storage and/or retrieval of information, such as a fixed disk drive 1154. Fixed disk drive 1154 may be a part of workstation 114 or may be separate and accessed through other interface systems. Many other devices can be connected such as the mouse 1156 connected to bus 1122 via serial port 1138, a modem 1157 connected to bus 1122 via serial port 1140 and the network interface 1158 connected directly to bus 1122. Modem 1157 may provide a direct connection to a remote server via a telephone link or to the Internet via an Internet Service Provider (ISP). Network interface 1158 may provide a direct connection to a remote server via a direct network link to the Internet via a

POP (point of presence). Network interface 1158 may provide such connection using various communication links, such as a dial-up wired connection with a modem, a direct link such as a T1, ISDN, or cable line, a wireless connection through a cellular or satellite network, or a local data transport system such as Ethernet or token ring over a local area network.

Many other devices or subsystems (not shown) may be connected in a similar manner (e.g., bar code readers, document scanners, digital cameras and so on). Conversely, it is not necessary for all of the devices shown in Fig. 1g to be present to practice various embodiments of the present invention. The devices and subsystems may be interconnected in different ways from that shown in Fig. 1g. The operation of a computer system such as that shown in Fig. 1g is readily known in the art and is not discussed in detail in this disclosure. Software code instructions to implement various embodiments of the present invention may be stored in computer-readable storage media such as one or more of system memory 1126, fixed disk 1154, CD-ROM 1152, or floppy disk 1148. Code instructions may also be implementd in various types of hardware circuits and firmware modules in addition to, or instead of, instructions implemented in software code. Additionally, workstation 114 may be any kind of computing device, and so includes personal data assistants (PDAs), network appliance, desktop, laptop, X-window terminal or other such computing devices. The operating system provided on workstation 114 may be MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, Linux® or other known operating system. Workstation 114 also supports a number of Internet access tools, including, for example, an HTTP-compliant web browser having a JavaScript interpreter, such as Netscape Navigator®, Microsoft Explorer® and the like.

The International Standardization Organization (ISO) has created a protocol layer model that distinguishes the typical tasks needed in communication. This model is called the Open Systems Interconnection (OSI) reference model 200 and is shown in Fig. 2a. This OSI protocol is used as an example protocol and is a representation of the various protocols currently in use. Fig. 2b is a subset of the OSI protocol in Fig. 2a known as the Internet Protocol (IP). Each protocol layer has a standard defined input and output, and provides clearly defined functions that can

improve connectivity between equipment provided by different manufacturing companies.

Referring to Fig. 2a, a user's content 202 is transformed through the layers into a bit stream 204 as it is transmitted through the network 100 (Fig. 1a). Each layer provides services to the layer above it, while shielding the upper level from functions performed below. Each layer can add a header and a trailer to the packet as the packet moves through the layers. The headers contain information that specifically addresses layer-to-layer communication. For example, the transport header (TH) includes information that only the transport layer uses. All other layers below the transport layer pass the transport header as part of the packet.

The application layer 206 (also referred to as layer 7) deals with printing, file transfer, remote terminal services, and directory browsing. Some user applications exist directly at the application layer 206, such as the known Telnet and FTP for file transfer protocol. Other user applications have application layer functions built into them. For example, a word processing program that can print to a network printer has application layer functions built into it.

The primary job of the presentation layer 208 (also referred to as layer 6) is that of translator. In presentation layer 208, operations such as translating ACSII into EBCIDIC, and vice versa, compression, decompression, encryption, and decryption are performed. Essentially, the presentation layer 208 transforms data into the form that the application layer 206 can accept.

Session layer 210 regulates the flow of information between applications. Session layer 210 synchronizes communication, and takes care of security and handling errors outside the scope of network communications, such as a server with a full disk drive, or a disk that needs to be inserted.

The objective of transport layer 212 (also referred to as layer 4) is to provide reliable data transmission for the layers above it. The transport layer 212 uses sequence numbers and flow control to keep information moving at the controlled rate, and to assure that the recipient knows how to reassemble an incoming stream of

data blocks in the correct order. The transport layer 212 also performs multiplexing; combining data to conserve bandwidth, or splitting a file into smaller data packets that can travel over several network pathways. The transport layer 212 can send a signal back to the upper layers when a transmission cannot get through.

Network layer 214 (also referred to as layer 3) deals with moving packets of information across a network. Large networks are made up of smaller sub-networks called segments. Within a segment two systems can communicate with each other just by referencing their layer two hardware addresses. To cross from one segment to another, systems need to know the network layer address of the destination system. Devices that operate on layer three of the network forward packets from one segment to the next based on the destination network address of the packet. They choose how to forward the packet by either dynamically determining the best route, or by looking up a route from a static table. Through this method a packet is routed one node at a time from its source, across the network, to its destination.

Data link layer 216 (also referred to as layer two) performs several tasks. It compiles the stream of ones and zeros coming from the physical layer 218 into bytes, and then into frames. The data link layer 216 can add its own header to the information it passes down to the physical layer 218. Information in the header usually includes the destination and source addresses of the frame. The data link layer 216 also detects and rejects corrupted frames and performs flow control.

Physical layer 218 (also referred to as layer one) transforms data to and from a signal on the network media and defines functionality of the network hardware including connector types, on/off signal voltages and durations to define a 1 or a 0, and whether the media is copper wire, optical fibers, or open air.

Content 202 can be in one of a variety of formats, such as documents created with a word processing program, image data, audio data, or a combination of audio and video data, to name a few. File formats can include their own control information regarding the data and the format of the data in the file.

As an example of a file format, Motion Picture Experts Group (MPEG-2) files can contain MPEG-2 compressed video, compressed audio, control data, and/or user data. The most basic file component is known as an Elementary Stream (ES) 302, 304, 306, 308. A program, such as a television program or a Digital Versatile Disk (DVD) track, contains a combination of elementary streams (typically one for video, one or more for audio, control data, subtitles, etc). Each ES 302, 304, 306, 308 output by an MPEG audio, video, and some data encoders contain a single type of signal that is usually compressed. There are various forms of ES 302, 304, 306, 308, including:

Digital Control Data,
Digital Audio (sampled and compressed),
Digital Video (sampled and compressed), and
Digital Data (synchronous, or asynchronous).

For video and audio, the data is organized into access units, each representing a fundamental unit of encoding. For example, in video, an access unit will usually be a complete encoded video frame.

Each ES 302, 304, 306, 308 is input to an MPEG-2 processor (e.g. a video compressor or data formatter) which accumulates the data into a Packetized Elementary Stream (PES) packet 310, an example of which is shown in Fig. 3a. The PES packet 310 may be a fixed or variable sized block. For example, one type of PES packet may include up to 65536 bytes per block and a 6 byte protocol header 312. The information in the protocol header 312 is, in general, independent of the transmission method used. A PES packet 310 usually is organized to contain an integral number of ES 302, 304, 306, 308, collectively referred to as a payload 314.

In one embodiment, the protocol header 312 includes a start code, a stream identifier (i.e., audio, video, of command/control identifier), and PES Indicators. The PES Indicators provide additional information about the stream to assist processing of the PES packet 310 including whether scrambling is used, the chosen scrambling method, priority of the current PES packet 310, whether the payload 314 starts with a video or audio start code, whether the payload 314 is copyright protected, whether the ES 302, 304, 306, 308 is original, and a set of optional fields,

which if present, are inserted before the start of the PES payload 314. The optional fields include presentation and decode time stamps, an Elementary Stream Clock Reference (ESCR), the rate at which the ES 302, 304, 306, 308 was encoded, trick mode, copyright information, Cyclic Redundancy Check (CRC), and PES extension information, which may be used to support MPEG-1 streams.

Referring to Fig. 3b, a transport stream 320 includes of one or more programs. Each program is defined as a collection or a multiplex of individual program elements that share the same time base. The transport bit stream comprises transport packets 322, 324 having 188 bytes each. The transport header 326 contains a Program ID (PID) to identify the contents of the packet, along with time stamps. The transport payload 328 encapsulates PES packet(s) 310 as well as dedicated transport packets, known as the Program Specific Information (PSI), which are set aside to identify the structure of the stream.

While Figs. 3a and 3b show the format for MPEG-2 files, files in one of many different known formats, and subsets of known formats, can be transported through network 100 (Fig. 1a) using the OSI reference model 200 (Fig. 2a). For example, MPEG Layer III (also referred to MP3), is a file format for the audio portion of MPEG files.

The communication protocol header and/or trailer for each layer, as well as the content 202 (Fig. 2a), can include content match information and control information. The DEDs 102 (Fig. 1a) search data packets for the content match information to determine whether transmission of data packets associated with a particular piece of content should be restricted. If transmission of associated data packets is restricted, then the control information can be used by the RTPs 128 (Fig. 1a) to determine which transaction(s) to process to control transmission of the data packets. While some of the header and trailer fields are designated for specific parameters, other fields can be allocated to allow the creator of the content 202 to include the control information. The control information can be unique to the creator, user, and/or content 202, and can be encrypted or unencrypted, or otherwise protected using any suitable means to help prevent users from accessing and changing the control information.

In one embodiment, the creator adds the content match information and the control information at application layer 206. The content match information is also supplied to DED 102 (Fig. 1a) as described hereinbelow. DED 102 can then search the transport streams 320 (Fig. 3b), also referred to as data packets, being transmitted through NAP 104 (Fig. 1a) to determine whether the data packets include the content match information. The content match information can be unique to the creator, user, and/or content 202, and can be encrypted or unencrypted, or otherwise protected using any suitable means to help prevent users from accessing and changing the content match information. The content match information can also be generated randomly, and DED 102 can be dynamically reprogrammed with the new, randomly generated content match information before the data packets are transmitted.

The content provider also can supply or indicate transaction instructions in the control information to be used in the RTP 128 when the DED 102 matches the content match information in a data packet. For example, if the user is required to pay for the content before receiving it, the RTP 128 transmits a transaction prompt that is displayed at the user's workstation 114 (Fig. 1a) informing the user of the price to be paid for the content, and allowing the user to accept or decline the purchase. As another example, the RTP 128 can transmit a prompt to inform the user that content infected with a virus is attempting to be transmitted from or received to the user's workstation 114, and that transmission or reception of the virus is being halted. As another example, the RTP 128 can transmit a prompt to inform the user that content subject to security control is attempting to be transmitted from or received to the user's workstation 114, and that transmission or reception of the confidential content is being halted. As a further example, the RTP 128 can tally statistics regarding transmission of designated content for purposes such as rating the popularity of the content.

Referring now to Fig. 4a, a flow diagram of an embodiment of a method for processing data packets in the network 100 (Fig. 1a) in accordance with an embodiment of the present invention is shown. Process 402 searches each data packet for content match information. DED 102 (Fig. 1a) can perform multiple

content matches on each data packet, as indicated by the series of processes 402. Each content match process 402 searches for content that meets the criteria of content match information supplied by various entities such as content providers, business organizations, and/or government organizations. Various functions can be performed based on the content, such as collecting payment for the authorized use of copyrighted content, preventing outgoing transmission of confidential material, preventing incoming receipt of material previously designated as unwanted by the recipient, and preventing the transmission of files containing viruses to the workstations 114 (Fig. 1a).

Process 402 can include logic to search for particular watermarks or fingerprints to identify copyright content based on the content match information from the content providers. It also can include logic to understand one or more hashing functions.

If content match information is not found in a data packet, process 402 forwards the data packet to its destination. If a content match is found in the data packet, process 404 determines whether the subject data packet is simply being monitored for statistical analysis or sampling. If so, process 405 updates the database 130 with the specified statistics or samples, and the data packet is transmitted to its destination.

When process 404 determines that the data packet is not just being monitored for statistical analysis or sampling, process 410 can temporarily store the incoming packets associated with the data packet for which a content match was found in buffer 412 while process 414 determines whether the RTP 128 should be invoked to process a transaction.

In one embodiment, process 414 queries database 130 to determine whether a transaction account for the user exists. A transaction account for a user can be established in many different ways. In one implementation, the transaction account for the user is established by the user's network service provider at the NAP 104. The user typically must pay a network service provider for access to the network 100 (Fig. 1a), and therefore the same billing account can be used with minimal overhead.

Alternatively, process 414 can allow the user to establish a transaction account by supplying electronic payment information, such as a credit or debit card number, a prepaid card number, or use an electronic wallet as known in the art.

If the user requesting the content that is being downloaded has established a transaction account, process 416 generates a notice that is presented to the user in process 418. Various types of prompts and messages can be generated by process 416 and presented to the user's workstation 114 (Fig. 1a) by process 418. The type of message or prompt depends on the transaction to be performed as indicated by the control information in the data packet. The control information is transmitted to the RTP 128 by the DED 102.

For example, process 416 can generate a prompt 450 such as shown in Fig. 4b to inform the user that they must agree to pay a fee to download the requested copyrighted content. The user can indicate their decision to either accept or decline the charge by selecting the "yes" or "no" options on the display. If the purchase was accepted, the user can provide electronic payment information, such as a credit card number, or check a box and provide a password or authorization code to authorize the charge to their established network service provider account.

As another example, process 416 can generate a prompt such as shown in Fig. 4c at workstations 114 (Fig. 1a) that allows the users to authorize a charge to an account, such as the transaction account established in process 414, or another account such as by supplying a different credit card number.

Fig 4i shows an example of a prompt that includes notice of a retail transaction from a participating retailer over the network 100 (Fig. 1a). The prompt includes shipping and handling information, and the amount of sales tax on the purchase, which is derived from a tax table stored in the RTP 128 (Fig. 1f).

Process 420 determines whether the user agreed to pay for the content. This can be implemented by monitoring the user's response to the notice that was sent in process 418. Process 422 processes the transaction if the user agrees to pay for the copyrighted material, and process 424 updates the database 130 with relevant

information regarding the transaction. Process 408 resumes transmission of the data packets from buffer 412 to their destination.

If process 420 determines that the client has not purchased the content, process 426 updates the database 130 with relevant information regarding the aborted download, and process 428 discards the data packets associated with the content.

Referring again to process 414, if a transaction account does not exist, process 430 generates a message, such as shown in Fig. 4d indicating that the content cannot be downloaded to the user's workstation because the content is protected and is not authorized for downloads or uploads.

Figs. 4e and 4f show examples of messages that can be generated by process 430 and presented by process 432 to the user's workstation to inform the user that the content is infected with a virus and therefore will not be downloaded or uploaded. In some embodiments, the user can choose an option (not shown) to attempt to clean the virus from the file using an anti-virus utility.

Fig. 4g shows an example of another message that can be generated by process 430 and presented by process 432 to the user's workstation to inform the user that they are attempting to upload secured information to the Internet and the transmission has been halted.

Fig 4h is an example of a message that can be generated by process 430 and forwarded to a system administrator to provide notice of an attempt to transmit content subject to security controls from one of the workstations 114 on the network 100 (Fig. 1).

Process 434 can be included to update database 130 to record information regarding the denial to transmit the content. Entries also can be made in database 130 that may be used to generate statistical information regarding the download attempts. This information in database 130 regarding the content also can be provided to and/or accessed by the owner of the content.

Process 436 ceases transmission of the content, and process 428 discards the data packets associated with the content. In one implementation, process 428 deallocates the memory occupied by the content's data packets in data buffer 412 to make the memory available to store other data packets.

In some implementations, processes 434 and 426 can give the user privacy options to withhold some or all of the user's information in database 130 from outside access and dissemination.

Referring now to Fig. 5a, a diagram of network 500 is shown that includes multiple NAPs 104 and DEDs 102 along the various levels of network 500 to provide a comprehensive system for controlling transmission of data packets through network 500. As shown in Fig. 5a, one or more DEDs 102 can be located at Level 1 Network Access Points (NAPs) where very high-speed data transfers are made, such as those achievable with OC-192/OC-48 connections, for example. DEDs 102 can also be located at Level 2 NAPs, Level 3 NAPs, Level 4 Internet Service Providers (ISPs), and Level 5 subnetworks. In some embodiments, Level 2 and Level 3 NAPs transfer data at rates that are slower than Level 1 NAPs, such as those achievable with OC-12/OC-192 connections, and OC-1/OC-48 connections, respectively, for example. At the Level 4 ISPs, data is transferred at still slower rates using infrastructure such as 56 K modems, T-1 or T-3 lines, DSL, and Ethernet connections. Level 4 connections are accessible by user workstations 114 at the Level 5 sub-networks. Other levels and sublevels of network 500 can be implemented at any of Levels 1 through 5 of network 500.

As shown in Fig. 5a, DEDs 102 can be located at one or more NAP and ISP at each level. Although not shown in Fig. 5a, DEDs 102 can also be located within a Level 5 subnetwork to prevent unauthorized swapping of files in peer-to-peer networks. A network that includes a DED 102 at each NAP 104 would check for content match information in the data packets transmitted on the network.

Fig. 5b shows DEDs 102 residing at multiple locations along routes for transmitting packets through network 505. For example, a DED 102 can be positioned between workstation 114 and NAP 104. DEDs 102 can also be positioned

between 2 NAPs 104. As an example of the utility of placing DEDs 102 at multiple levels in network 505, when a user at workstation 114 in St. Louis sends data packets to a user at a workstation 114 in Chicago, DED 102' checks for content match information in the data packets, thereby preventing unauthorized transmission of data between the users. DEDs 102 can also be used to facilitate authorized distribution of information, however. For example, DEDs 102 can allow the user in St. Louis, who owns a copy of copyrighted content, to post the content on a website that can be accessed by the user in Chicago. When the user in Chicago downloads a copy of the content, DED 102 can facilitate a transaction whereby the user in Chicago authorizes payment to the copyright owner in exchange for being able to receive a copy of the content from the website provided by the user in St. Louis.

Another example of the utility of placing DEDs 102 at multiple locations in network 505 is shown at NAPs 104 associated with Company X, which includes Campuses A, B, and C NAPs, two or more Departments NAPs at Campuses A and C, and multiple user workstations 114 connected to Department NAPs. DED 102'' resides at Company X NAP and can prevent transmission of unauthorized information outside of Company X from any user workstation 114. Similarly, DED 102''' is located at Campus C's NAP to protect certain data from being transmitted outside Department A on Campus C.

Fig. 5c shows a block diagram of multiple DEDs 102 in a network 510. Since multiple DEDs 102 can be installed throughout the network 510, data packets are likely to encounter more than one DED 102 during transmission through the network 510. The DEDs 102 can communicate with each other as described in the following paragraphs in order to prevent more than one prompt being presented to the user for the same packet, or set of packets associated with the same content.

When the sending DED 102A matches content in a data packet with content match information, the sending DED 102A generates and transmits a message that includes information to generate a prompt to the user at the destination workstation 114D. In some embodiments, the message includes information such as an identifier for the DED 102D closest along the route to workstation 114D, an identifier of the content, a flow identifier that indicates the network route between the sending DED

102A and the receiving DED 102D, the control information for the content, and an identifier for the RTP 128 associated with DED 102D. DED 102B, which is further along the route to workstation 114D, interprets the message from the sending DED 102A and transmits the message to the next downstream DED 102C. The message is transmitted to each downstream DED along the route until the message reaches the destination DED 102D. The destination DED 102D transmits a message to inform the workstation 114D of the potential transaction. In response, the workstation 114D transmits the message to the RTP 128 along with an identifier of the workstation 114D.

The identifier for the workstation 114D is unique to allow the RTP 128 to send the prompt, such as shown, for example, in Figs. 4b-4i, to the workstation 114D. The information presented in the prompt is based on the transaction to be performed. For example, a prompt 450 shown in Fig. 4b informs the user at the workstation 114D that the content requested is subject to copyright protection and must be paid for before it can be downloaded to the user. The prompt 450 includes data entry windows and selectable options that allow the user to indicate whether they accept or decline to purchase the content at workstation 114D. If the user agrees to the price and the terms, the transaction is authorized at the RTP 128. The RTP 128 conducts the required transaction and sends a Release_Content or Cease_Content transmission message to the DED 104D, depending on whether the content was authorized to be downloaded to the destination workstation 114D.

To prevent each DED 102D, 102C, 102B from performing a content match on the same packet, DED 102D forwards the message to all upstream DEDs 102C, 102B, 102A. If a Release_Content message is received, the DED 102A places a Release_Content identifier in the packet to indicate that the content is approved for transmission and then transmits the packet. The downstream DEDs 102B, 102C, and 102D along the route in the network 510 recognize the Release_Content identifier and transmit the packet without performing another content match, or generating another prompt, for the same packet.

If the Cease_Content transmission message is received, the originating DED 102A will not transmit the packet and clears the packet from its buffer

The Release_Content identifier indicating that the content is approved for transmission can be any combination of data that the DEDs are programmed to recognize as indicating that the packet can be transmitted with a content match. For example, the Release_Content identifier can be a setting of one or more bits in the header or trailer of the packet, or in the packet's payload. The identifier can be encrypted or decrypted, or implement other security mechanisms known in the art. Notably, the Release_Content identifiers and location in the packets can be updated or modified periodically to minimize the likelihood of users successfully transmitting unauthorized content by adding similar Release_Content identifiers to the packets. The Release_Content identifier can also include time/date stamp to indicate that the packet is authorized to be transmitted only within a certain time period of the time/date stamp.

Referring now to Figs. 5d and 5e, Fig. 5d shows a series of packets within a TCP stream transmitted from sending workstation 114A to destination workstation 114D may not take the same path through network 520 due to redundant paths and the load sharing capabilities of the routers 108 (Fig. 1a). More than one packet associated with the same content can therefore be subject to content matching at different DEDs. To prevent multiple content matches for related packets, when the DED 102A matches the content match information, the DED 102A buffers all of the packets associated with the content, and transmits a message along the route to the DED 102D associated with the destination workstation 114D. The message can include the control information, identifiers, as well as other information. In Fig. 5d, for example, DED 102D notifies the workstation 114D, the workstation 114D transmits the message along with its identifier to the RTP 128, and the RTP 128 conducts the required transaction. Once the transactions, if any, associated with the message have been processed by the RTP 128, the RTP 128 sends the Release_Content or Cease_Content message to the DED 102D, depending on whether the content was authorized to be downloaded to the destination workstation 114. DED 102D forwards the message to all upstream DEDs 102C, 102B, 102A, 102E. The Release_Content message includes an identifier for the TCP stream so that the packets authorized for transmission can be identified by each DED along the

various routes in the network 520 and allowed to continue without generating another prompt for the same packets.

Fig. 5e shows an example where there is no DED at NAP 104A for the sending workstation 114A. The content is therefore matched downstream after the packets have taken multiple paths. In this example, content can be matched at DED 102C and DED 102E. Each of these DEDs 102C and 102D will generate and send a Message through the receiving workstation to the RTP 128 for processing. The RTP 128 sends a Release_Content or Cease_Content message prompt to the closest DED 102D to the receiving workstation 114D. DED 102D forwards the message to all upstream DEDs that are buffering packets associated with that particular TCP stream.

Fig. 5f shows an embodiment of a system in which one or more of the DEDs 102A, 102B, 102C, 102D monitor packets for content as the packets are transmitted from workstation 114A to workstation 114D. In this embodiment, the control information in the packets indicates that the packets can be transmitted without generating a prompt at workstation 114D. As the DEDs match content in the packets, they transmit a message to notify the corresponding RTP 128. The message includes information to identify the packet. The RTPs 128 forwards the information to the CSBS 900. This information can be collected for a number of purposes including analyzing the number of times a piece of content is transmitted over the network, and the general vicinities of the sending and receiving workstations 114A, 114D.

Fig. 6a shows an example of a reprogrammable content match device 600 that can be used to implement at least a portion of DED 102 for use in network 100 in accordance with some embodiments of the present invention. Such a content match device 600 is available from the Field Programmable Port Extender (FPX) Project developed in the Applied Research Laboratory, Department of Computer Science, Washington University, St. Louis, Missouri, and further described in the publication entitled "Field Programmable Port Extender (FPX) for Distributed Routing and Queuing" by John W. Lockwood, Jon S. Turner, David E. Taylor, ACM

International Symposium on Field Programmable Gate Arrays (FPGA 2000), Monterey, CA, February 2000, pp. 137-144.

Content match device 600 utilizes Field Programmable Gate Arrays (FPGAs) to provide the performance advantage of Application-Specific Integrated Circuits (ASICs) to implement customized pipelines and perform parallel logic functions. FPGAs also can be reprogrammed to perform a content matching function.

As shown in Fig. 6a, content match device 600 includes two FPGA devices: one to implement a Network Interface Device (NID) 602 and another to implement a reprogrammable application device (RAD) 604. Content match device 600 is connected to network 100 (Fig. 1a) via switch 106 and line card 606. By performing all computations in FPGA hardware, cells and data packets can be processed at the full line speed of the line card 606.

The RAD 604 includes modules 608, 610 that implement the module-specific functionality. Each module 608, 610 on the RAD 604 connects to a Static Random Access Memory (SRAM) 612, 614, respectively, and to a wide synchronous dynamic RAM (SDRAM) 616, 618, respectively. The SRAM 612, 614 typically is used for applications that perform table lookup operations, while the SDRAM 616, 618 typically is used for applications such as packet queuing that transfers bursts of data and can tolerate higher memory latency.

The RAD 604 communicates with the NID 602 using a suitable interface 620, 622, such as the known Universal Test And Operation Physical Interface (UTOPIA) for Asynchronous Transfer Mode (ATM) transmission. Data packets transmitted over the interface 620, 622 are segmented into a sequence of fixed-size cells that are formatted as Internet Protocol (IP) over ATM, as known in the art. Each interface 620, 622 can include a small amount of buffering and implement flow control. A Start of Cell (SOC) signal is asserted at the input of the modules 608, 610 to indicate the arrival of data. The Transmit Cell Available (TCA) signal is asserted back toward an incoming data source to indicate downstream congestion. A method for communicating data between RAD 604 and NID 602 suitable for use in content match device 600 is described in Lockwood et al. U.S. Patent Application No.

_____ entitled TCP-Splitter: Reliable Packet Monitoring Methods and Apparatus For High Speed Networks, which is assigned to Washington University in St. Louis, Missouri, and is incorporated herein by reference.

The NID 602 controls the flow of data packets to and from the modules 608, 610. NID 602 also provides mechanisms to dynamically reprogram the modules 608, 610 over the network 100 (Fig. 1a). The combination of these features allows modules 608, 610 to be dynamically loaded and unloaded without affecting the switching of other traffic flows or the processing of packets by the other modules in the network 100.

As shown in Fig. 6b, the NID 602 includes several components that can be implemented in FPGA hardware. The components in NID 602 include: a four-port switch 630 to transfer data between ports 632, 634, 636, and 638; Virtual Circuit lookup tables (VC) on each port 632, 634, 636, 638 to selectively route flows; a Control Cell Processor (CCP) 640 to process control cells that are transmitted and received over the network 100 (Fig. 1a); programming interface logic 642 to reprogram the FPGA hardware on the RAD 604; and synchronous and asynchronous interfaces (not shown) to the four network ports 632, 634, 636, 638.

The CCP 640 can be implemented in hardware to manage the operation of the content match device 600 and to communicate over the network 100 (Fig. 1a). On the ingress interface from the switch 106, the CCP 640 listens and responds to commands that are sent on a specific virtual circuit. The NID 602 processes commands that include: (1) modification of per-flow routing entries; (2) reading and writing of hardware status registers, (3) reading and writing of configuration memory, and (4) commands that cause the logic on the RAD 604 to be reprogrammed. After executing each command, the NID 602 returns a response in a control cell.

In order to reprogram the RAD 604 over the network 100 (Fig. 1a), the NID 602 implements a suitable protocol to fill the contents of the on-board RAM with configuration data that is sent over the network 100. As each cell arrives, the NID 602 uses the data and the sequence number in the cell to write data into the RAD

Program in SRAM 644. Once the last cell has been correctly received, and the NID 602 holds an image of the reconfiguration byte stream that is needed to reprogram the RAD 604. At that time, another control cell can be sent to the NID 602 to initiate the reprogramming of RAD 604 using the contents of the RAD Program in SRAM 644.

The content match device 600 supports partial reprogramming of the RAD 604 by allowing configuration streams to contain commands that program only a portion of the logic on the RAD 604. Rather than issue a command to reinitialize the RAD 604, the NID 602 writes the frames of reconfiguration data to the RAD's reprogramming port via programming interface 642. This feature enables module 610 on the RAD 604 to continue processing packets during the partial reconfiguration. A suitable method for reprogramming the RAD 604 via content match device 600 to search a data stream for predefined patterns is described in Lockwood et al. U.S. Patent Application No. 10/152,532 entitled Methods, Systems, And Devices Using Reprogrammable Hardware For Highspeed Processing Of Streaming Data To Find A Redefinable Pattern And Respond Thereto, which is assigned to Washington University, St. Louis, Missouri, and is incorporated herein by reference.

In some embodiments, the DED 102 can be implemented using a combination of hardware, software, and/or firmware. A software-based DED can include a routing chip and an embedded processor that executes a kernel operating system. Any suitable combination of processor and operating system may be used.

Fig. 7 shows examples of system architectures that can be implemented to process transactions in accordance with an embodiment of the present inventions. One implementation includes a local NAP 104A communicating with RTP 128A, workstation 114A, and DED 102A. The workstation 114A communicates with the RTP 128A after receiving a prompt. For payment transactions, for example, the RTP 128A calculates all fees and costs and transmits a message to the workstation 114A that specifies the amount of the transaction. When DED 102A communicates with RTP 128A in a local region, workstation 114A communicates with the local RTP

128A after receiving a prompt. Thus, a local RTP 128A can process transactions in the local community.

The second implementation can include one or more regional RTPs 128B that communicate with local and remote workstations 114B and multiple NAPs 104B in a region. For example, the second implementation can include one RTP 128B to communicate with every NAP 104B in a metropolitan area. RTP 128B would be considered a local RTP. In an area with less population, one RTP 128B may be able to handle the NAPs 104B in an entire portion of a state. In this situation, RTP 128B would be considered a regional RTP.

Fig. 8a shows one implementation of the communication process between the DED 102, the workstation 114, and the RTP 128. After the workstation 114 has sent a request for content that is copyright protected, for example, the DED 102 finds a content match and/or the control information which identifies the content in one or more of the arriving packets as being copyright protected. In this situation, the process includes the following steps:

Step 1. DED 102 transmits a message to the workstation 114. The message includes information including an identifier for the DED 102 closest along the route to workstation 114, an identifier of the content, a flow identifier, the control information for the content, and an identifier for the RTP 128 associated with DED 102.

Step 2. Workstation 114 initiates a transaction notice to the RTP 128 that includes the identifier of the content, the control information for the content, an identifier of the workstation 114, and the identifier of the DED 102.

Step 3. The RTP 128 determines transaction costs, tax rates, and billing account information using in the transaction notice and in the database 130.

Step 4. The RTP 128 transmits a purchase prompt to the user at the workstation 114, such as shown in Fig. 4a or Fig. 4b.

Step 5. The user at the workstation 114 inputs a purchase decision.

Step 6. The purchase decision is transmitted to the RTP 128.

Step 7. The RTP 128 processes payment if the user authorized the purchase.

Step 8. The RTP 128 sends a Release_Content notice to the DED 102 if payment was authorized. If the user declines the purchase, the RTP 128 sends a Cease_Content notice to DED 102 to discontinue transmission of the content and discard the packets associated with the content.

Fig. 8b shows an example of a process for initializing communication between the workstation 114, the DED 102, and the RTP 128 including the following steps:

Step 1. The user at the workstation 114 invokes a network browser. The browser transmits a startup message to the DED 102. The DED 102 forwards the startup message to the RTP 128.

Step 2. The RTP 128 transmits an acknowledgment of the message to the DED 102.

Step 3. The DED 102 transmits an acknowledgement to the workstation 114 when the DED 102 is ready to perform content matches on packets.

Fig. 8c shows an embodiment of a process for preventing content containing confidential information from being transmitted over a network 100 (Fig. 1) from the workstation 114 including the following steps:

Step 1. The user at workstation 114 attempts to transmit secured content over the network. The secured content includes content match information that identifies the content as being subject to security controls and therefore should not be transmitted.

Step 2. The DED 102 recognizes the content match information indicating that the content should not be transmitted over the network 100 (Fig. 1). The DED 102 transmits a prompt, such as shown in Fig. 4g, to the workstation 114 to inform the user of the attempt.

Step 3. The DED 102 transmits a prompt, such as shown in Fig. 4h, to a systems administrator workstation 114 to inform the administrator of the attempt and provide an identifier of the workstation 114 and/or the user logged on to the workstation 114.

Step 4. The DED 102 transmits a message to the RTP 128 that includes information, such as the file attempting to be transmitted, the date and time of the attempt, and the identifiers for the workstation 112 and/or the user. The RTP 128 stores the information on storage system 142 (Fig. 1b).

Fig. 8d shows an embodiment of a process for halting transmission of computer viruses from the network 100 (Fig. 1) to the workstation 114. Once a virus has been identified, the DEDs 102 can be programmed with content match information that identifies files infected the virus. The process includes:

Step 1. The DED 102 performs a content match and detects the content match information indicating the file is infected with a virus.

Step 2. The DED 102 transmits a prompt, such as shown in Fig. 4e, to workstation 114 to inform the user of the infected file.

Step 3. The DED 102 updates the RTP 128 with information regarding the attempt to transmit the virus. The RTP stores the information on its storage system 142 (Fig. 1b), and the information can be used by system administrators for purposes such as determining the source of the virus.

Fig. 8e shows an embodiment of a process for halting transmission of (computer) viruses from the workstation 114 to the network 100 (Fig. 1). Once

again, when a virus has been identified, the DEDs 102 can be programmed with content match information that identifies files infected with the virus. The process includes:

Step 1. The DED 102 performs a content match and detects the content match information indicating the file is infected with a virus.

Step 2. The DED 102 transmits a prompt, such as shown in Fig. 4f, to workstation 114 to inform the user of the infected file.

Step 3. The DED 102 updates the RTP 128 with information regarding the attempt to transmit the virus. The RTP 128 stores the information on its storage system 142 (Fig. 1b), and the information can be used by system administrators for purposes such as disinfecting the files on all of the local workstations and storage systems.

Application programs to support the processes described for Figs. 8a-8e on the workstations 114 can be provided to the workstations 114 via downloads from selected sites on the network 100 (Fig. 1), or distributed by the NAPs 104. The browser program on the workstation 114 can execute the application programs through an application program interface, as known in the art. The application programs also can be incorporated in later versions of the browser. The application programs include functions for receiving messages containing the prompts from the RTPs and DEDs, presenting the prompts to the user at the workstation 114, and initializing communication between the RTPs 128 and the DEDs 102.

Fig. 9 shows a Central Storage and Backup Systems (CSBS) 900 communicating with RTPs 128. All transactional information, monitoring information, and RTP operational information is forwarded to the CSBS 900 to backup all information and monitor the operability of every RTP 128. If an RTP 128 becomes inoperable, the CSBS 900 can transmit information to re-route all DEDs 102 associated with the inoperable RTP 128 to another RTP 128.

Fig. 10 shows a Content Matching Server (CMS) 1000 that can transmit updated content match information to all DEDs 102, at regular intervals or as

required. This includes new content match information as well as removing or modifying obsolete content match information. One or more CMSs 1000 may be co-located with the CSBS 900 (Fig. 1a) or located in regional offices and connected to network 100 (Fig. 1a).

Fig. 11 shows a representation of a Point of Purchase (POP) 1100 that allows local and state governments to collect sales tax on sales transactions conducted via the network 100. The transactions are processed at the RTP 128 and a prompt summarizing the cost of the goods or services from the vendor, and the sales tax added, is presented to the user at workstation 114. The RTP 128 uses look-up tables 158, such as shown in Fig. 1f and/or a formula to calculate the appropriate tax rates for the transactions. The RTP 128 can transmit a payment prompt, such as shown in Fig. 4i, showing the total cost of the transaction to the workstation 114. The RTP 128 can bill the appropriate billing system once the user approves the purchase at the workstation 114. The amount of sales tax to charge depends on the state and/or local government in which the workstation 114 is located. Thus an identifier that provides the location of the workstation 114 can be used to determine the amount of sales tax to add to a sales transaction.

A system and method in accordance with an embodiment of the present invention establishes a new data enabling point at the NAPs 104 (Fig. 1a) that will non-intrusively facilitate the management of data packets transmitted on the network 100. The utility and advantages of such a system and method include:

Facilitating the protection of any digital content that is copyright-protected. The DED 102 can be implemented at local NAPs 104, or at the NAP 104 of the content provider, to prompt the user for payment of the content. Transmission of copyright-protected content ceases at the NAP 104 unless the user agrees to pay for the content.

Providing facilities for collecting and tabulating information regarding designated digital content downloaded or streamed in real time for ratings services and statistical analysis.

Establishing a new virus protection point for all users connected to the NAP 104. This protection point can be updated universally to prevent viruses from moving off the network backbone and through the NAPs 104.

Providing facilities to prevent confidential information from being transmitted past the NAP 104 and onto the network 100.

Moving the Point of Purchase (POP) to a NAP 104 on the local level.

Providing the capability to add taxes and tariffs on transactions subject to taxation as the transactions are processed by the RTP 128.

Facilitating the ability of users to purchase digital content from any workstation 114 on the network 100.

Including the DED 102 at the NAP 104 establishes processes and facilities for monitoring data to and from all users at a common access control point. This enables a series of transactions or actions to be triggered depending on the content match information in the data packets. This applies to protecting digital copyright content, sales transactions for content, and confidential or sensitive information such as medical, financial, and industrial information, computer virus protection, and numerous other security applications.

Further, if the use of a standard encryption scheme is agreed to, the DEDs 102 can monitor encrypted packets for compliance with the standard. A network 100 in accordance with an embodiment of the present invention can prevent transmission of encrypted files that do not conform to the standard encryption scheme over network 100.

The foregoing detailed description has set forth various embodiments of the present invention via the use of schematic diagrams and examples. It will be understood by those within the art that each schematic diagram component and operations and/or components illustrated by the use of examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or any combination thereof.

The above description is intended to be illustrative of the invention and should not be taken to be limiting. Other embodiments within the scope of the present invention are possible. For example, a system and method in accordance with an embodiment of the present invention can utilize a network transport model other than the OSI model (Fig. 2b). Further, the Data-Enabling Device (DED) could take the form of software running over existing hardware switching systems located at the NAP. Variations and modifications of the embodiments disclosed herein can be made based on the description set forth herein, without departing from the spirit and scope of the invention as set forth in the following claims.

WHAT IS CLAIMED IS:

1. A system for controlling transmission of data packets through an information network, comprising:

a Regional Transaction Processor (RTP); and

a data Enabling Device (DED) operable to:

receive at least one data packet from the information network,

detect when the at least one data packet includes content match information, and

issue a message to a workstation and invoke the RTP to process a transaction when the content match information is detected in the at least one data packet.

2. The system as set forth in claim 1, wherein the transaction processed is based on the content match information.

3. The system, as set forth in claim 1, wherein the DED is operable to detect when the at least one data packet includes content match information at a rate proportional to the rate at which the data packets are received.

4. The system, as set forth in claim 1, wherein the DED prevents further transmission of the at least one data packet based on the content match information.

5. The system, as set forth in claim 1, wherein the RTP comprises a network server and a database, and is operable to process transactions for requests for content.

6. The system, as set forth in claim 1, wherein the DED is located at a network access point (NAP).

7. The system, as set forth in claim 1, further comprising a plurality of DEDs along a network route, wherein each DED is operable to communicate with at least one of the other DEDs.

8. The system, as set forth in claim 7, wherein the plurality of DEDs include a first DED that generates a message and at least one intermediate DEDs operable to forward the message to the DED closest to the workstation along the network route.

9. The system, as set forth in claim 7, wherein the plurality of DEDs are operable to communicate with each other to prevent transmitting more than one message for the same data packet through the network route.

10. The system, as set forth in claim 1, wherein the RTP transmits a Release_Content or Cease_Content message to the DED, based on whether the at least one data packet was authorized to be downloaded to the workstation.

11. The system, as set forth in claim 1, wherein the DED includes Field Programmable Gate Arrays (FPGAs).

12. The system, as set forth in claim 11, wherein the FPGAs can be reprogrammed over the network to perform a content matching function.

13. The system, as set forth in claim 11, wherein a portion of the DED can be dynamically reprogrammed and the DED is operable to continue processing the data packets during the partial reprogramming.

14. The system, as set forth in claim 1, further comprising a Central Storage and Backup System (CSBS) operable to communicate with the RTP, to monitor operation of the RTP, and to store transaction information.

15. The system, as set forth in claim 14, wherein the CSBS is operable to transmit information to reprogram the DED to communicate with another RTP.

16. The system, as set forth in claim 1, further comprising a content matching server operable to store content match information, to communicate with the DED, and to transmit the content match information to the DED.

17. The system, as set forth in claim 1, wherein the DED is operable to suspend transmission of the data packets through the information network until a response to a prompt is received.

18. A method for controlling transmission of identifiable content over an information network, comprising:

providing content match information for the content to a DED, wherein the DED is located in the information network along a transmission path of a plurality of data packets, wherein at least one data packet includes the content match information;

receiving the at least one data packet in the DED;

detecting the content match information in the at least one data packet in the DED; and

issuing a prompt to a workstation based on the content match information when the content match information is detected in the at least one data packet.

19. The method as set forth in claim 18, wherein the prompt is based on the content match information.

20. The method, as set forth in claim 18, further comprising preventing further transmission of the at least one data packet based on the content match information.

21. The method, as set forth in claim 18, further comprising processing a transaction based on a user's response to the prompt.

22. The method, as set forth in claim 18, further comprising transmitting a message among a plurality of DEDs along the transmission path to prevent transmitting more than one prompt for the same data packet.

23. The method, as set forth in claim 18, further comprising processing a transaction based on the content match information, and transmitting a Release_Content or Cease_Content message to the DED based on whether content was authorized to be downloaded to the workstation during the transaction.

24. The method, as set forth in claim 18, further comprising reprogramming a portion of the DED to detect different content match information.

25. The method, as set forth in claim 18, further comprising suspending transmission of the at least one data packet through the information network until a response to the prompt is received.

26. A computer program product comprising:
program instructions to implement the method of claim 18.

27. A data signal comprising:
program instructions to implement the method of claim 18.

28. An apparatus for controlling transmission of identifiable content over an information network, comprising:
means for providing content match information for the content to a DED, wherein the DED is located in the information network along a transmission path of a plurality of data packets, wherein at least one data packet includes the content match information;
means for receiving the at least one data packet in the DED;
means for detecting the content match information in the at least one data packet in the DED, and
means for issuing a prompt to a workstation based on the content match information when the content match information is detected in the at least one data packet.

29. The apparatus as set forth in claim 28, further comprising means for generating the prompt based on information in the at least one data packet.

30. The apparatus, as set forth in claim 28, further comprising means for preventing further transmission of the at least one data packets based on information in the at least one data packet.

31. The apparatus, as set forth in claim 28, further comprising means for processing a transaction based on a user's response to the prompt.

32. The apparatus, as set forth in claim 28, further comprising means for transmitting a message among a plurality of DEDs along the transmission path to prevent transmitting more than one prompt for the same packet.

33. The apparatus, as set forth in claim 28, further comprising means for processing a transaction based on the content match information, and means for transmitting a Release_Content or Cease_Content message to the DED based on whether content was authorized to be downloaded to the workstation during the transaction.

34. The apparatus, as set forth in claim 28, further comprising means for reprogramming a portion of the DED to detect different content match information.

35. The apparatus, as set forth in claim 28, further comprising means for suspending transmission of the at least one data packet through the information network until a response to the prompt is received.

36. An apparatus for controlling transmission of data packets in an information network, comprising:

a Regional Transaction Processor (RTP) operable to communicate with a Data Enabling Device (DED) and at least one workstation, wherein the DED is operable to detect content match information in at least one of the data packets, and further wherein the RTP comprises:

instructions operable to generate information to include in a prompt to be presented at the workstation, wherein the prompt is based on information in the at least one data packet.

37. The apparatus as set forth in claim 36, wherein the DED is operable to detect the content match information at a rate proportional to the rate at which the data packets are received.

38. The apparatus, as set forth in claim 36, wherein the DED is operable to prevent further transmission of the data packets based on the information in the at least one data packet.

39. The apparatus, as set forth in claim 36, wherein the RTP further comprises instructions operable to process a transaction based on the information in the at least one data packet.

40. The apparatus, as set forth in claim 36, wherein a plurality of DEDs are positioned along a network route, and further wherein each DED is operable to communicate with at least one of the other DEDs.

41. The apparatus, as set forth in claim 40, wherein the plurality of DEDs include a first DED that generates a message and at least one intermediate DED operable to forward the message to the DED closest to the workstation along the network route.

42. The apparatus, as set forth in claim 40, wherein the plurality of DEDs are operable to communicate with each other to prevent transmitting more than one message for the same data packet through the network route.

43. The apparatus, as set forth in claim 39, wherein the RTP is further operable to transmit a Release_Content or Cease_Content message to the DED, based on whether the at least one data packet was authorized to be downloaded to the workstation during the transaction.

44. The apparatus, as set forth in claim 36, wherein a portion of the DED can be dynamically reprogrammed and the DED is operable to continue processing packets during the partial reprogramming.

45. The apparatus, as set forth in claim 39, wherein the RTP is operable to communicate with a Central Storage and Backup System (CSBS), wherein the CSBS is operable to monitor operation of the RTP, and to store transaction information.

46. The apparatus, as set forth in claim 45, wherein the CSBS is operable to transmit information to reprogram the DED to communicate with another RTP.

47. The apparatus, as set forth in claim 36, wherein the RTP is operable to communicate with a content matching server, wherein the content matching server is operable to store content match information, to communicate with the DED, and to transmit the content match information to the DED.

48. The apparatus, as set forth in claim 36, wherein the DED is further operable to suspend transmission of the at least one data packet through the information network until a response to the prompt is received.

49. An apparatus comprising:

a Central Storage and Backup System (CSBS) operable to communicate with a plurality of Regional Transaction Processors (RTPs) and to provide backup storage for the RTPs, wherein the RTPs are operable to communicate with a Data Enabling Device (DED) and at least one workstation, wherein the DED is operable to detect content match information in at least one data packet, and further wherein the RTP comprises:

instructions operable to generate information to include in a prompt to be presented at the workstation, wherein the prompt is based on information in the data packet.

50. The apparatus, as set forth in claim 49, wherein CSBS is further operable to monitor the operation of the RTPs.

51. The apparatus, as set forth in claim 49, wherein the CSBS stores transaction information for the RTPs.

52. The apparatus, as set forth in claim 49, wherein the CSBS maintains the content match information.

53. A computer program product comprising:

instructions to enable communication between a workstation, a Data Enabling Device (DED), and a Regional Transaction Processor (RTP), wherein the DED is operable to detect content match information in at least one data packet and to prevent further transmission of other data packets based on the information in the at least one data packet, and further wherein the RTP is operable to generate information to include in a prompt to be presented at the workstation, wherein the prompt is based on information in the at least one data packet.

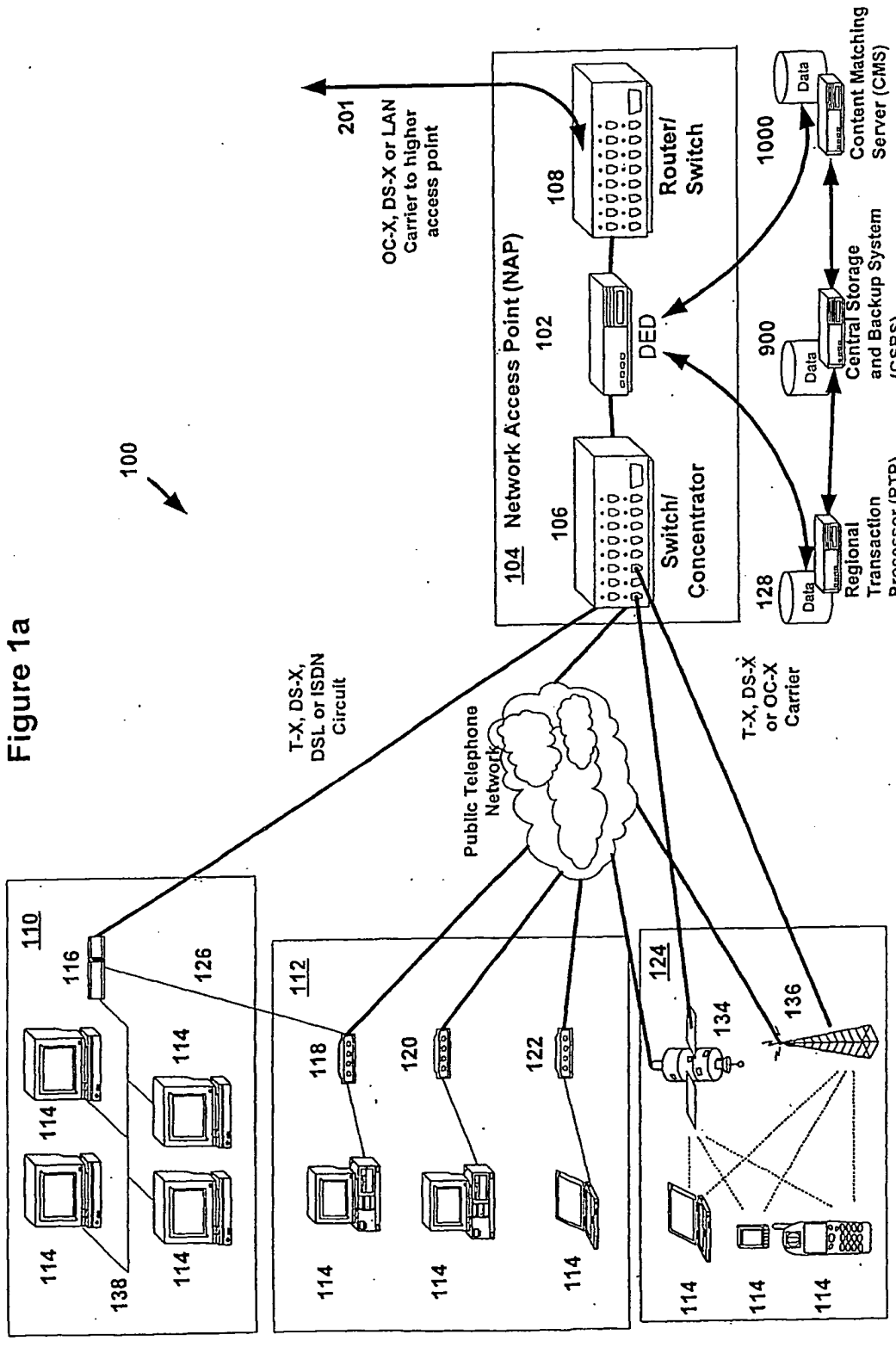

100
201
OC-X, DS-X or LAN Carrier to higher access point
104 Network Access Point (NAP)
102
DED
108
Router/ Switch
106
Switch/ Concentrator
1000
Data
Content Matching Server (CMS)
900
Data
Central Storage and Backup System (CSBS)
128
Data
Regional Transaction Processor (RTP)
T-X, DS-X, DSL or ISDN Circuit
Public Telephone Network
T-X, DS-X or OC-X Carrier
110
116
126
114
138
112
118
120
122
124
134
136

Figure 1a

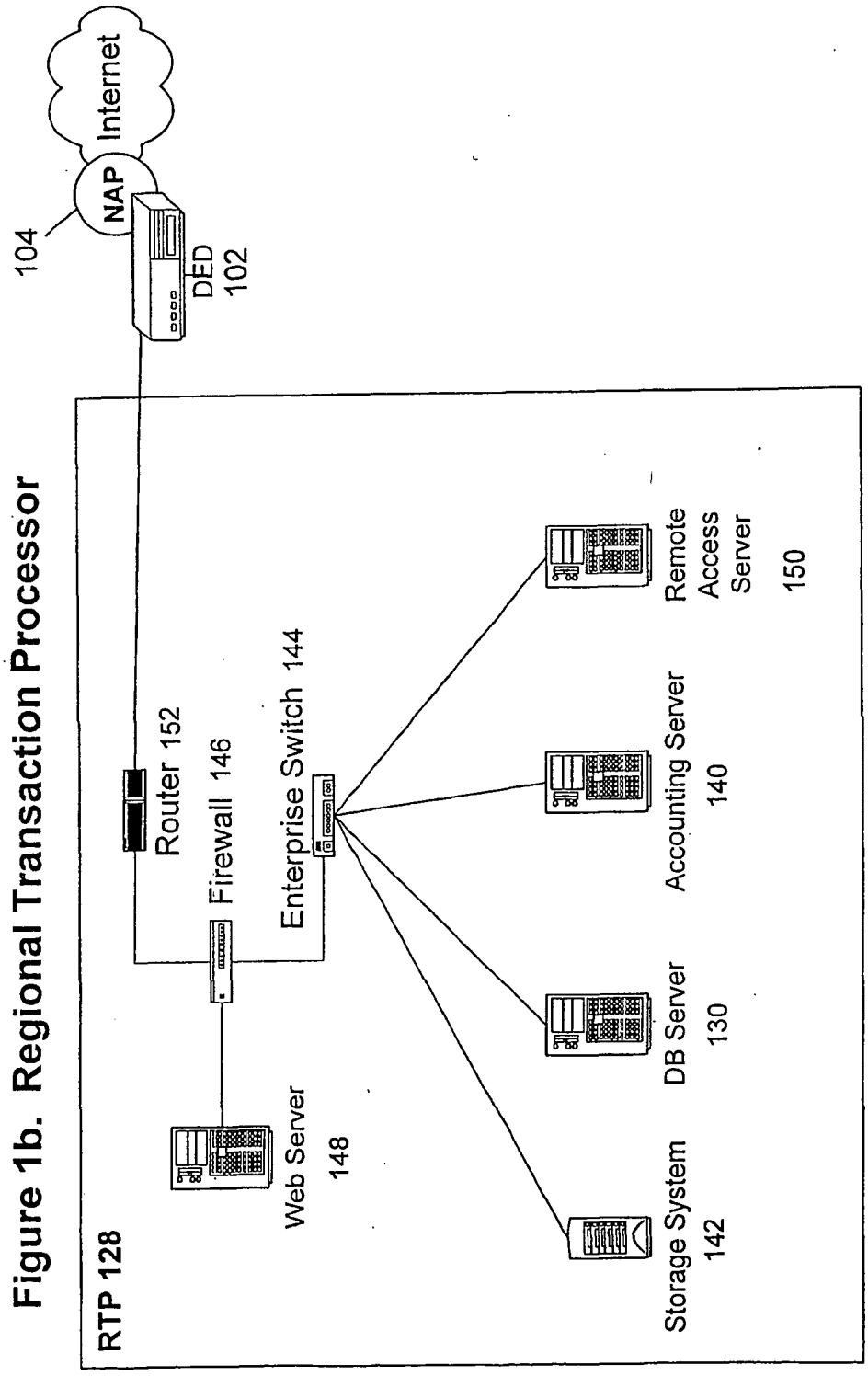
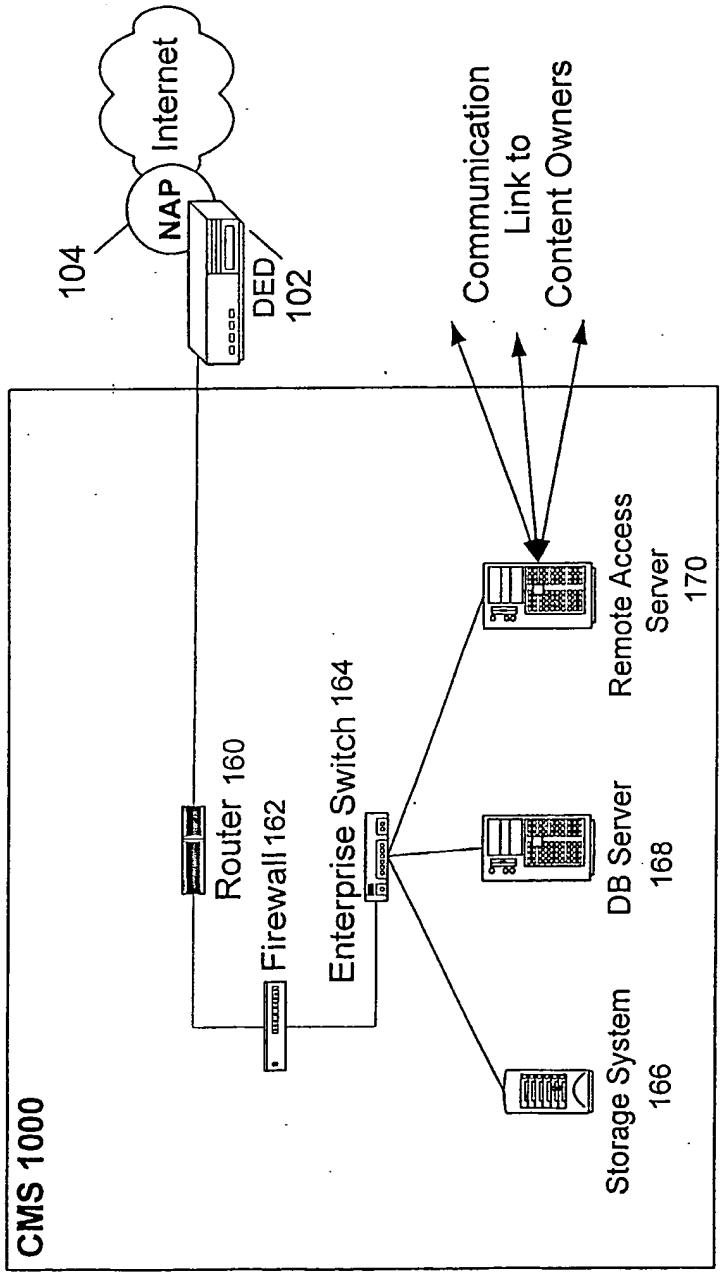


Figure 1b. Regional Transaction Processor

Figure 1c. Content Matching Server



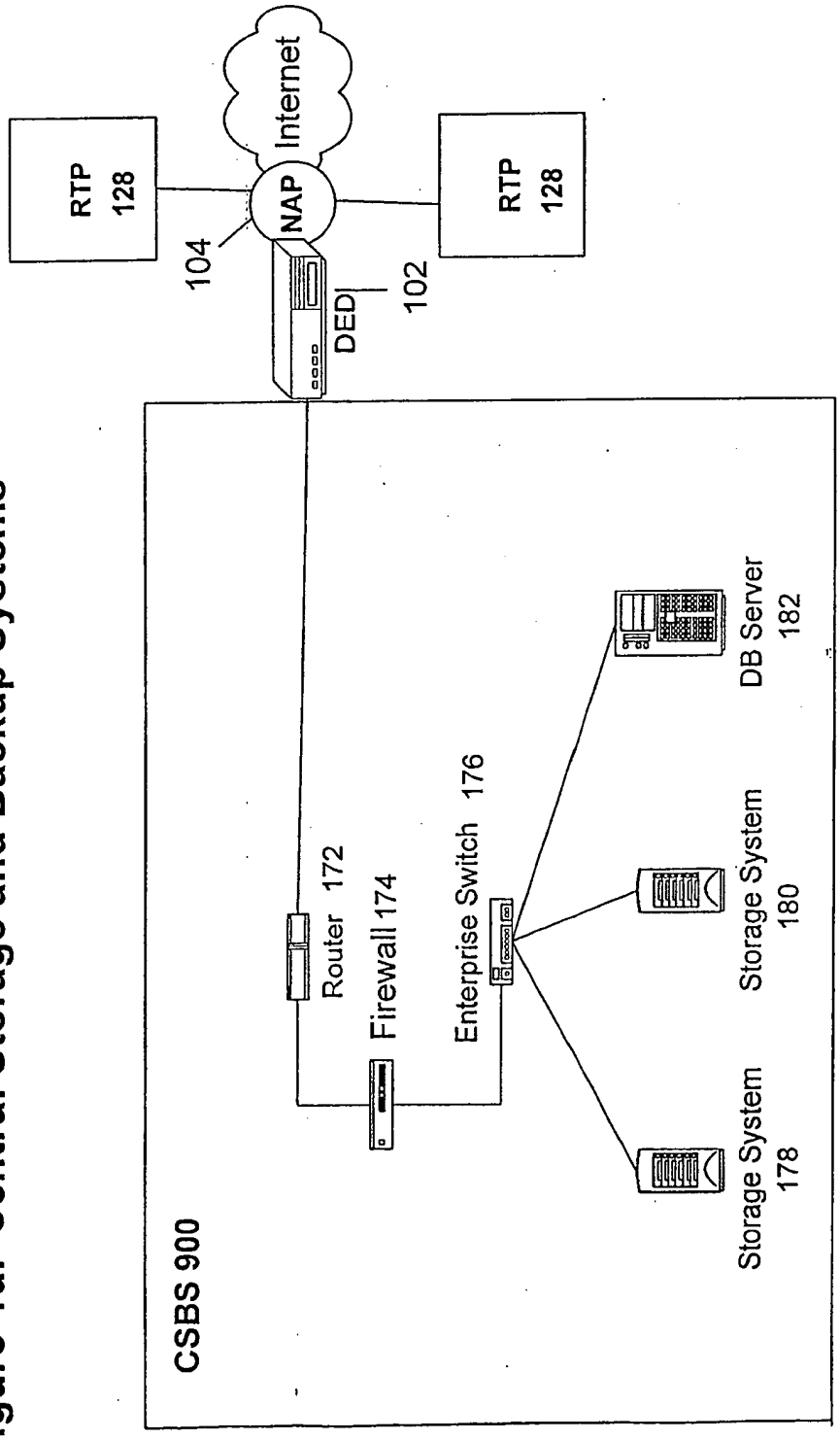


Figure 1d. Central Storage and Backup Systems

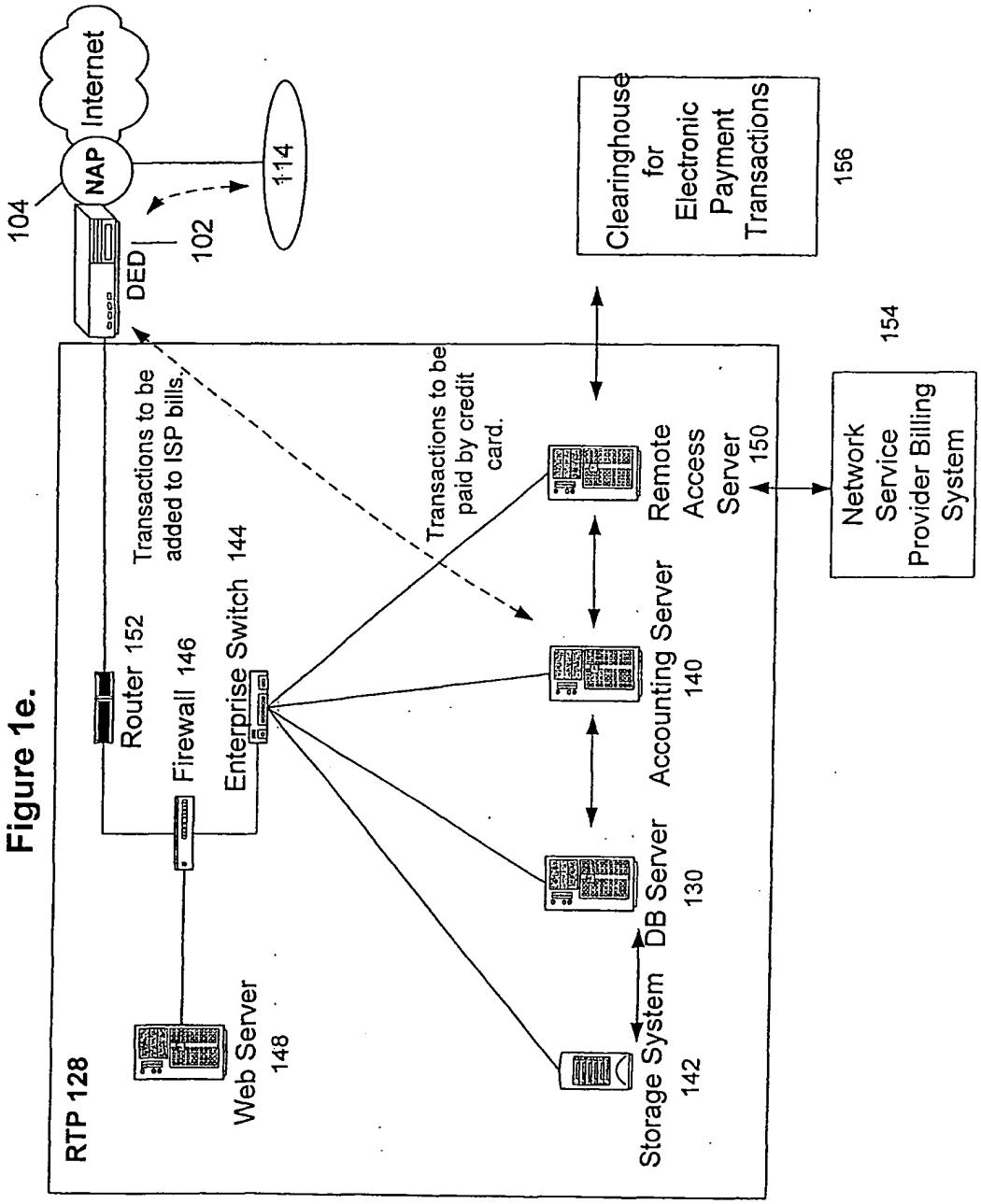

Internet
NAP
104
DED
102
114
Clearinghouse for Electronic Payment Transactions
156
154
Network Service Provider Billing System
Transactions to be added to ISP bills.
Transactions to be paid by credit card.
Remote Access Server 150
Accounting Server 140
DB Server 130
Storage System 142
Router 152
Firewall 146
Enterprise Switch 144
Web Server 148
RTP 128

Figure 1e.

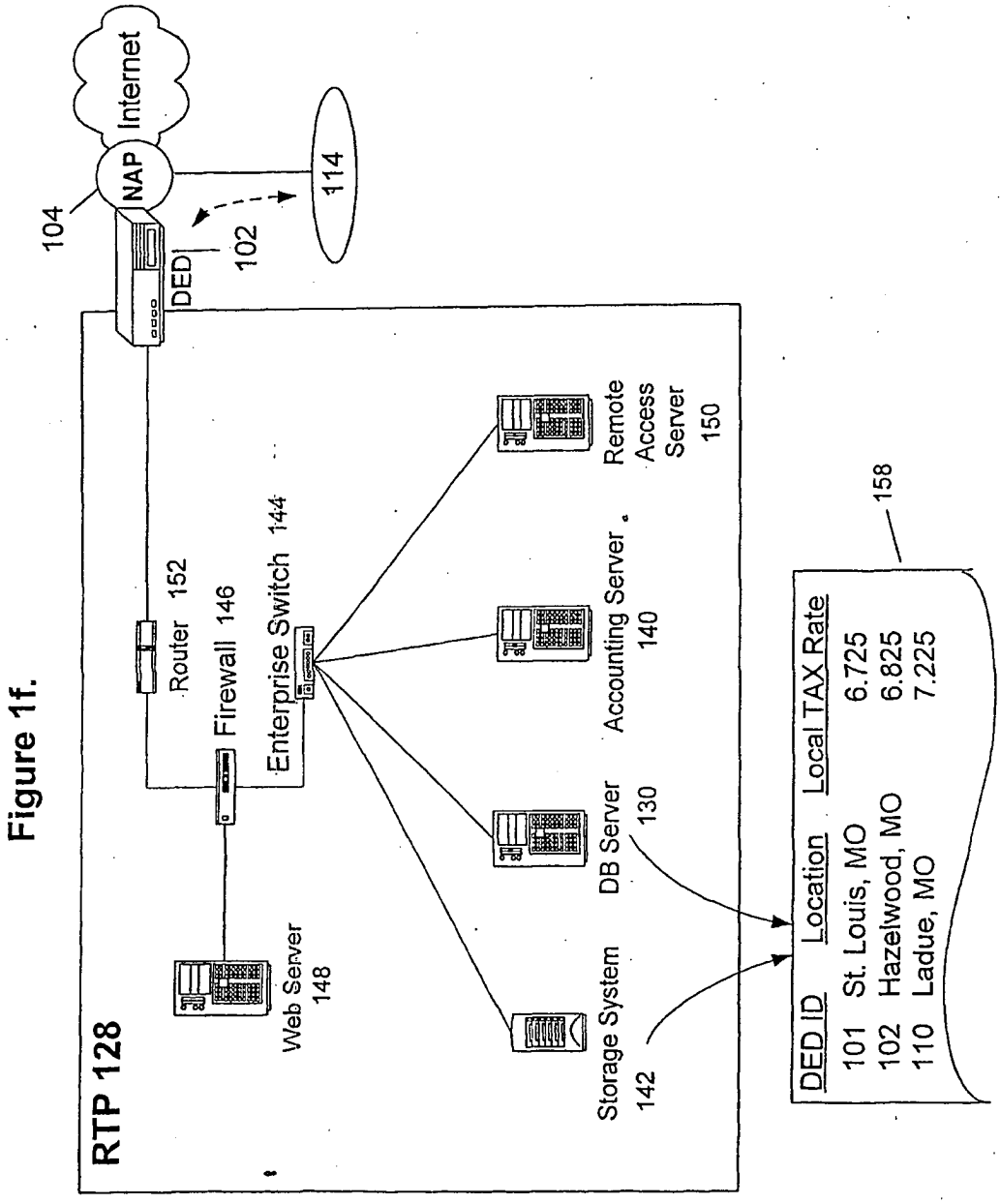

Internet
NAP
104
DED
102
114
RTP 128
Router 152
Firewall 146
Enterprise Switch 144
Web Server 148
Storage System 142
DB Server 130
Accounting Server 140
Remote Access Server 150
158
DED ID Location Local TAX Rate
101 St. Louis, MO 6.725
102 Hazelwood, MO 6.825
110 Ladue, MO 7.225

Figure 1f.

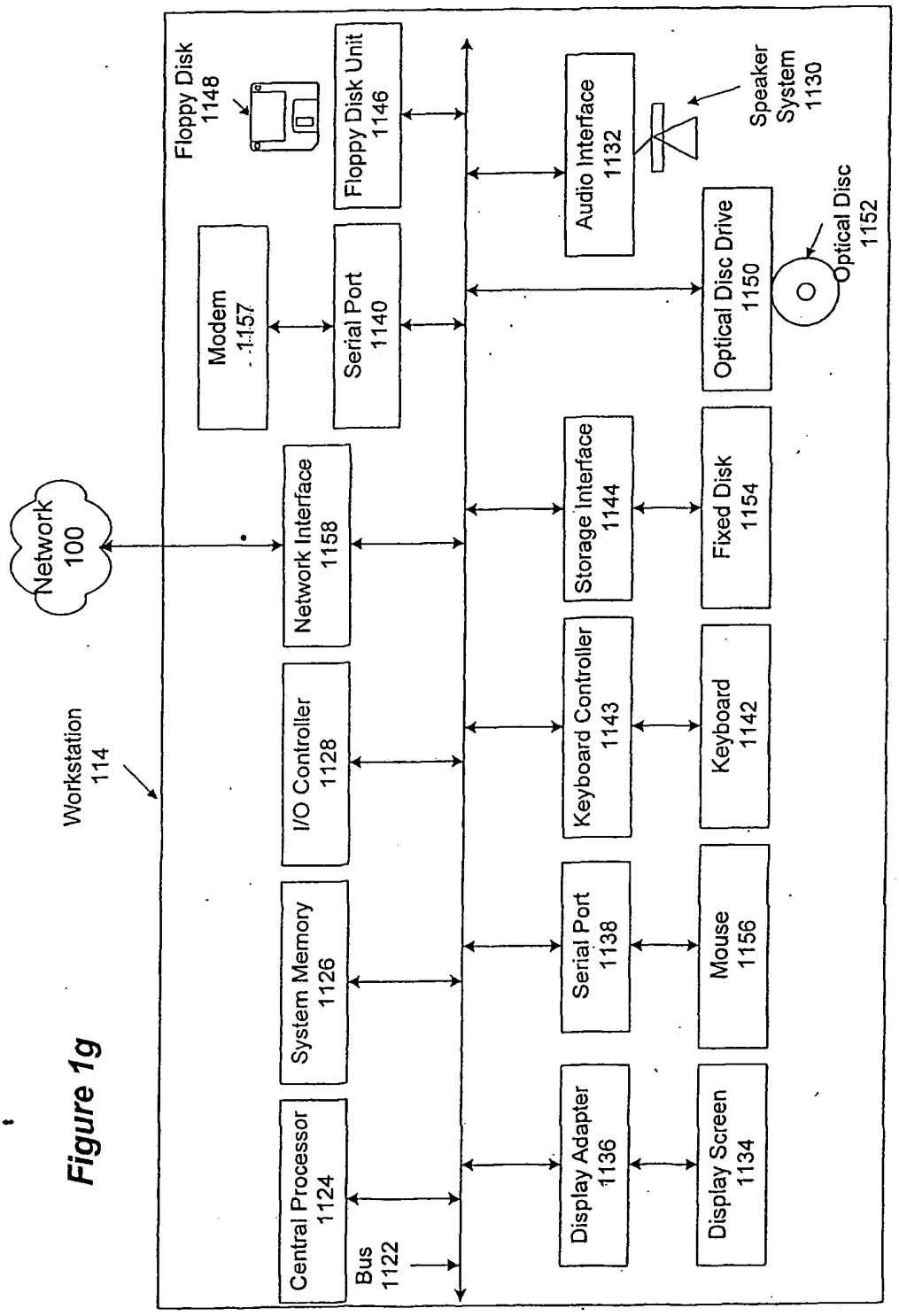

Network
100
Workstation
114
Central Processor
1124
Bus
1122
System Memory
1126
I/O Controller
1128
Network Interface
1158
Modem
1157
Floppy Disk
1148
Serial Port
1140
Floppy Disk Unit
1146
Audio Interface
1132
Speaker
System
1130
Optical Disc Drive
1150
Optical Disc
1152
Storage Interface
1144
Fixed Disk
1154
Keyboard Controller
1143
Keyboard
1142
Serial Port
1138
Mouse
1156
Display Adapter
1136
Display Screen
1134

Figure 1g

Figure 2a

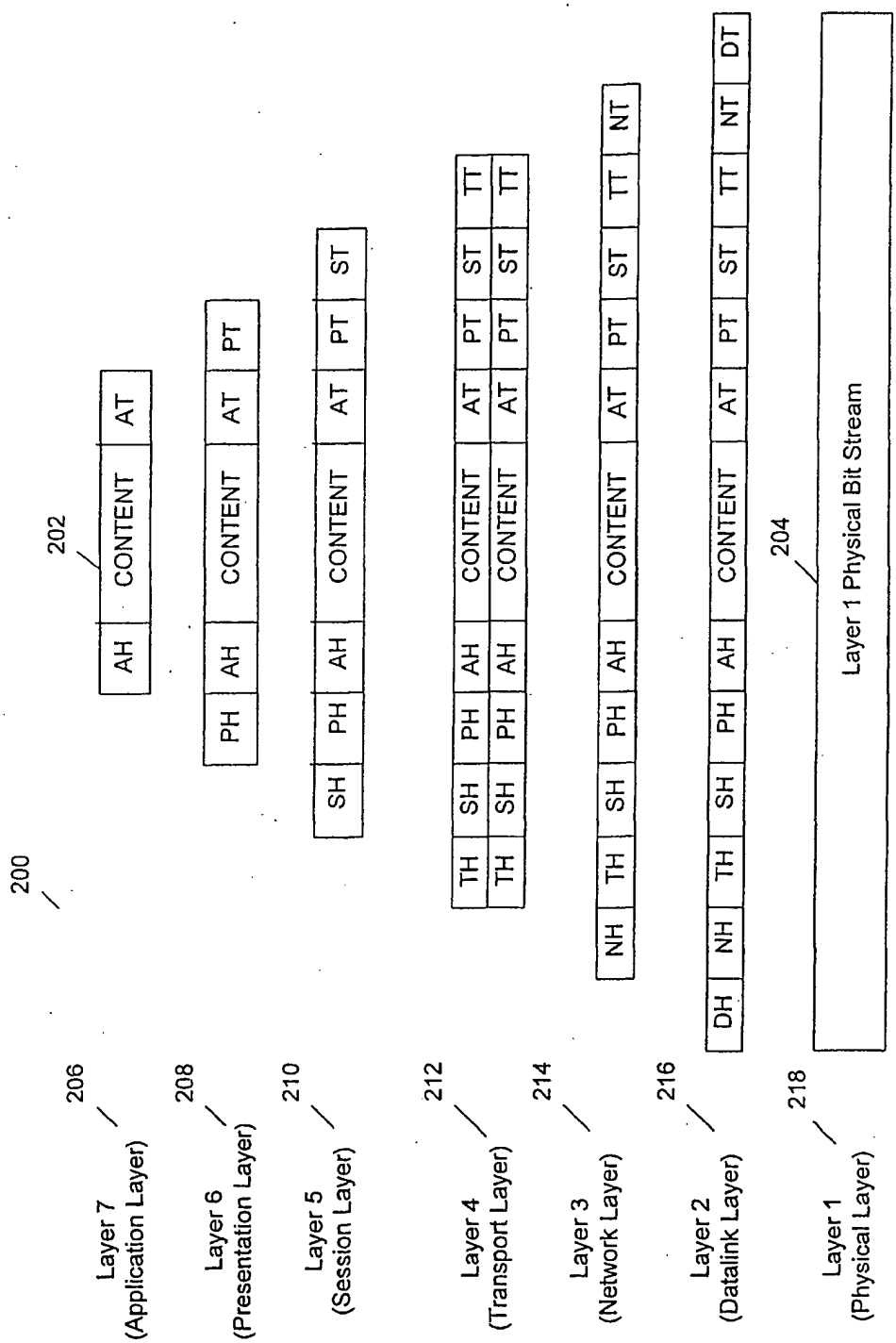
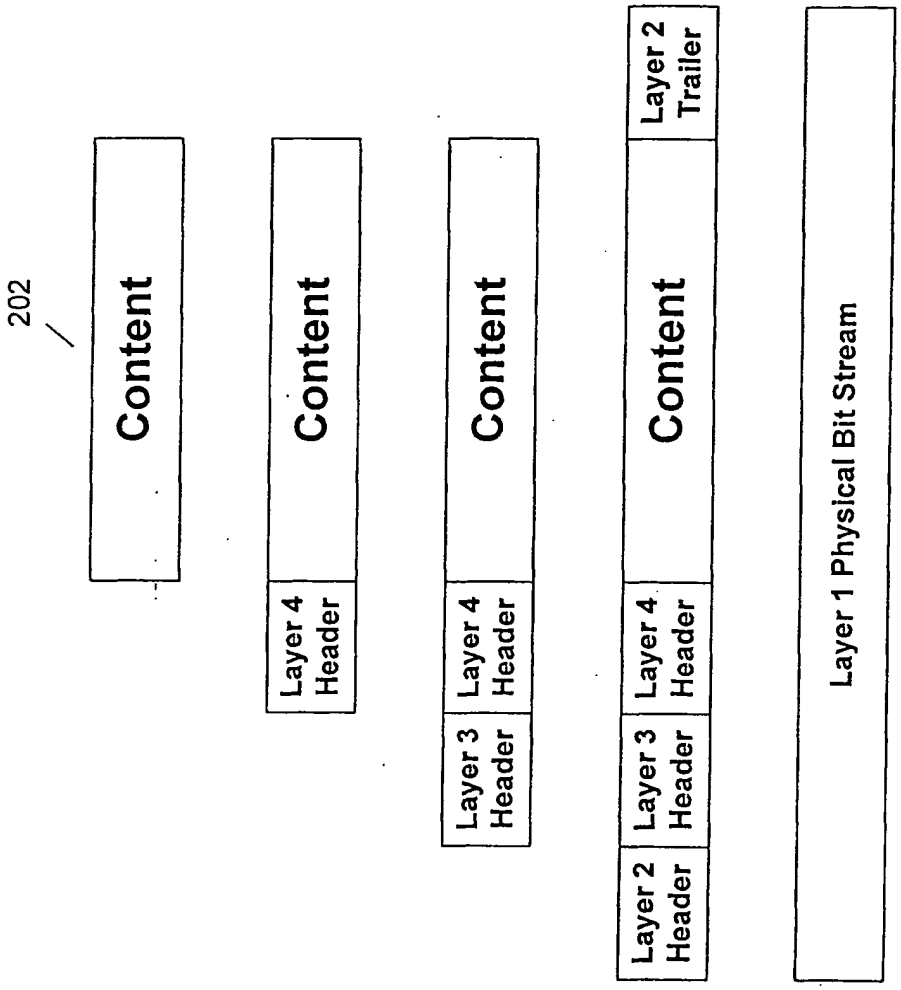

200
202
AH
CONTENT
AT
PH
AH
CONTENT
AT
PT
SH
PH
AH
CONTENT
AT
PT
ST
TH
SH
PH
AH
CONTENT
AT
PT
ST
TT
TH
SH
PH
AH
CONTENT
AT
PT
ST
TT
NH
TH
SH
PH
AH
CONTENT
AT
PT
ST
TT
NT
DH
NH
TH
SH
PH
AH
CONTENT
AT
PT
ST
TT
NT
DT
204
Layer 1 Physical Bit Stream
206
Layer 7
(Application Layer)
208
Layer 6
(Presentation Layer)
210
Layer 5
(Session Layer)
212
Layer 4
(Transport Layer)
214
Layer 3
(Network Layer)
216
Layer 2
(Datalink Layer)
218
Layer 1
(Physical Layer)

Figure 2b. Layered Data Encapsulation Process



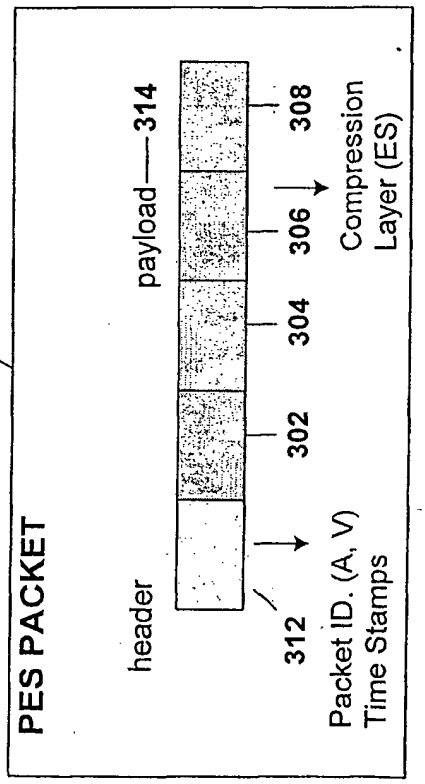

310
PES PACKET
header
payload
314
312
302
304
306
308
Packet ID. (A, V)
Time Stamps
Compression
Layer (ES)

Fig. 3a

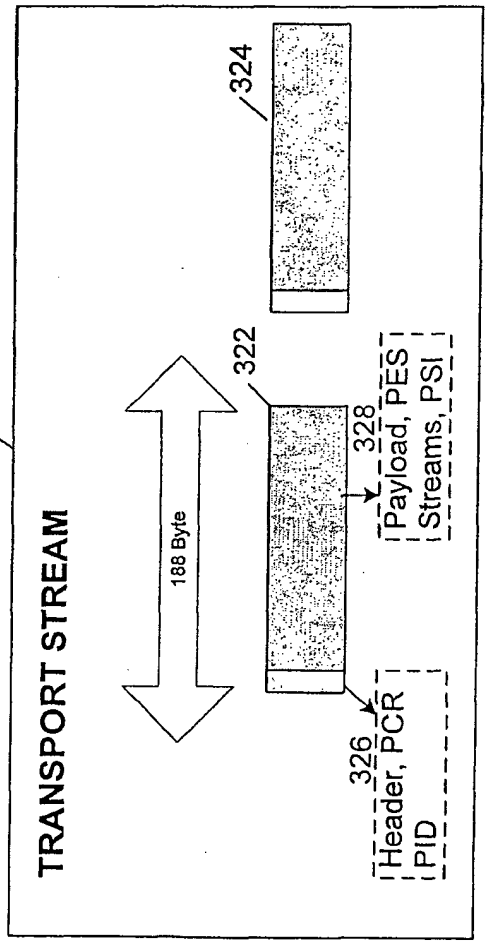

320
TRANSPORT STREAM
188 Byte
322
324
326
328
Header, PCR
PID
Payload, PES
Streams, PSI

Fig. 3b

Figure 4a

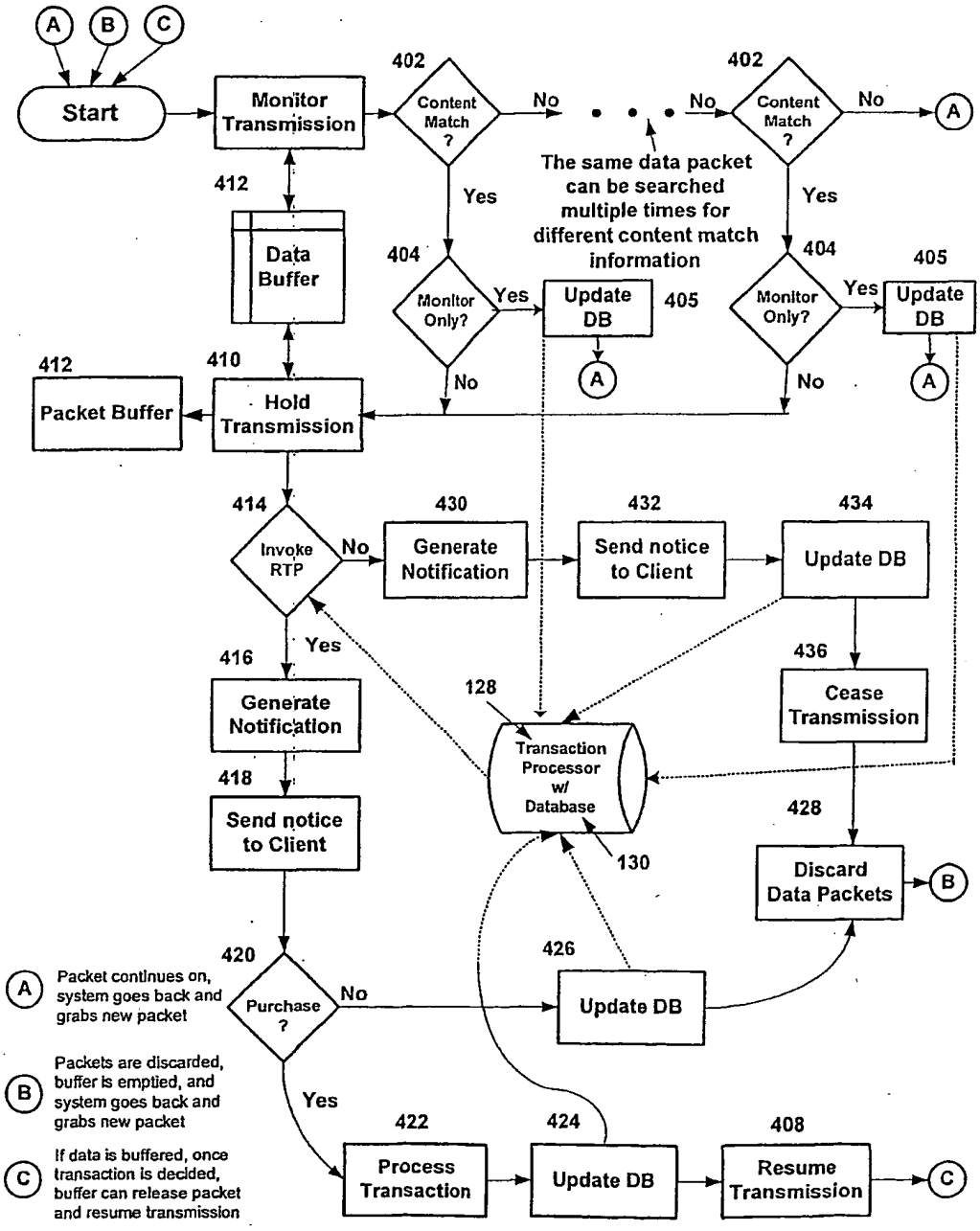

A
B
C
Start
Monitor Transmission
402
Content Match ?
No
The same data packet can be searched multiple times for different content match information
Yes
404
Monitor Only?
Update DB
405
412
Data Buffer
410
Hold Transmission
Packet Buffer
414
Invoke RTP
430
Generate Notification
432
Send notice to Client
434
Update DB
416
Generate Notification
418
Send notice to Client
128
Transaction Processor w/ Database
130
436
Cease Transmission
428
Discard Data Packets
420
Purchase ?
426
Update DB
422
Process Transaction
424
Update DB
408
Resume Transmission
A Packet continues on, system goes back and grabs new packet
B Packets are discarded, buffer is emptied, and system goes back and grabs new packet
C If data is buffered, once transaction is decided, buffer can release packet and resume transmission

Figure 4B

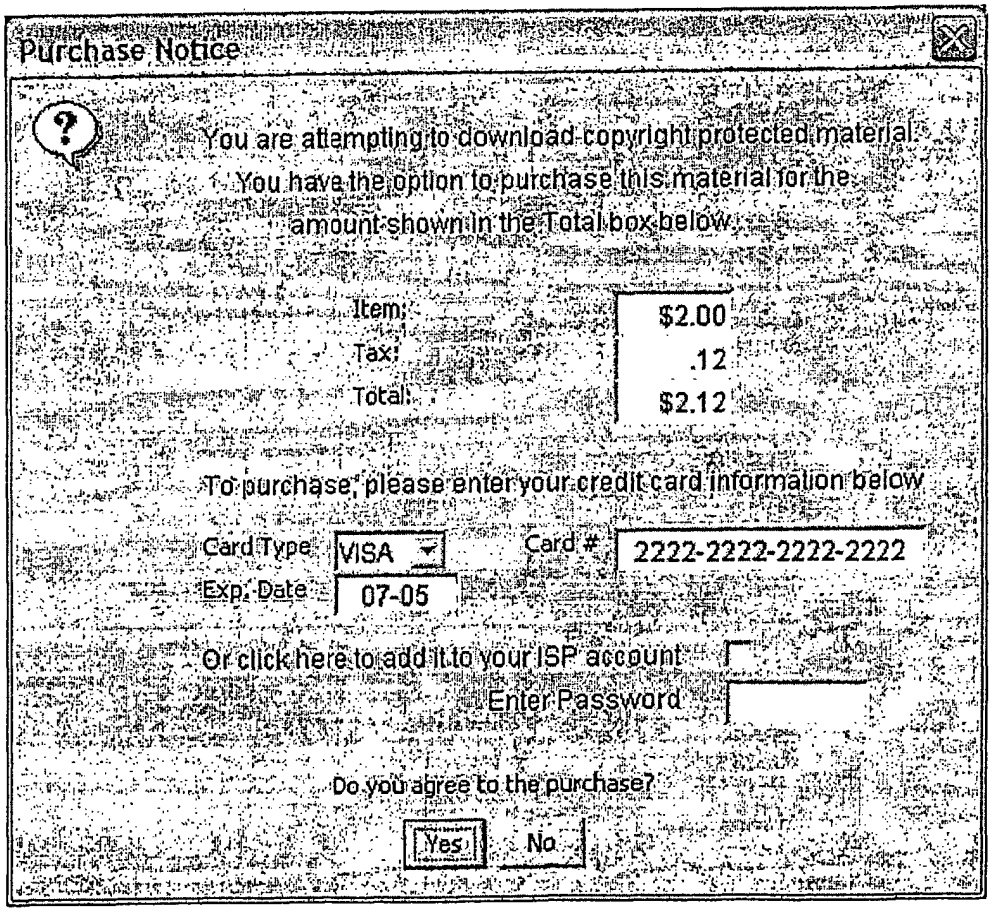

Purchase Notice
You are attempting to download copyright protected material.
You have the option to purchase this material for the amount shown in the Total box below.
Item:
$2.00
Tax:
.12
Total:
$2.12
To purchase, please enter your credit card information below
Card Type:
VISA
Card #:
2222-2222-2222-2222
Exp. Date:
07-05
Or click here to add it to your ISP account
Enter Password
Do you agree to the purchase?
Yes
No

Fig. 4C

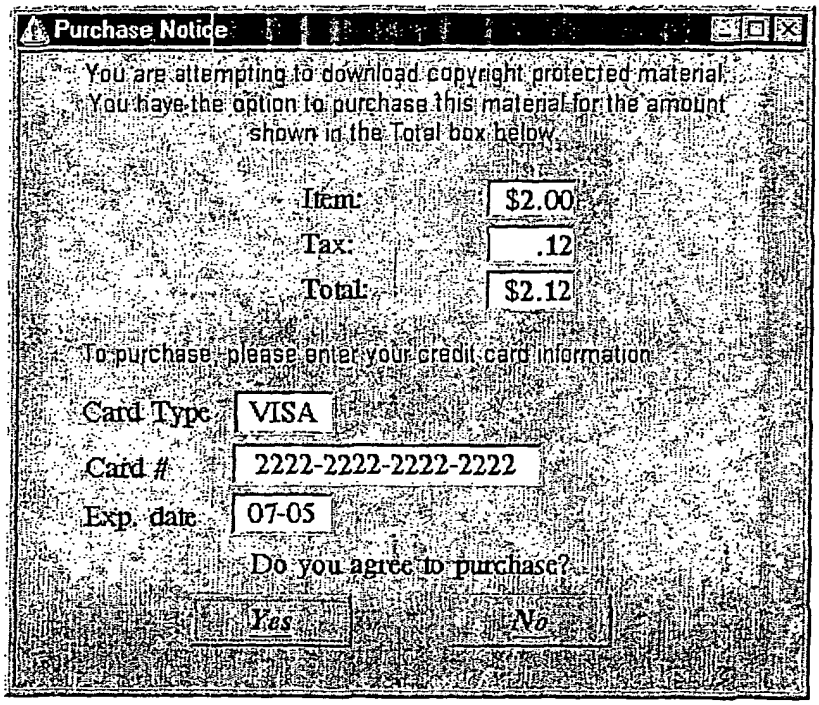

Purchase Notice
You are attempting to download copyright protected material.
You have the option to purchase this material for the amount
shown in the Total box below.
Item: $2.00
Tax: .12
Total: $2.12
To purchase, please enter your credit card information.
Card Type: VISA
Card #: 2222-2222-2222-2222
Exp. date: 07-05
Do you agree to purchase?
Yes
No

Figure 4D

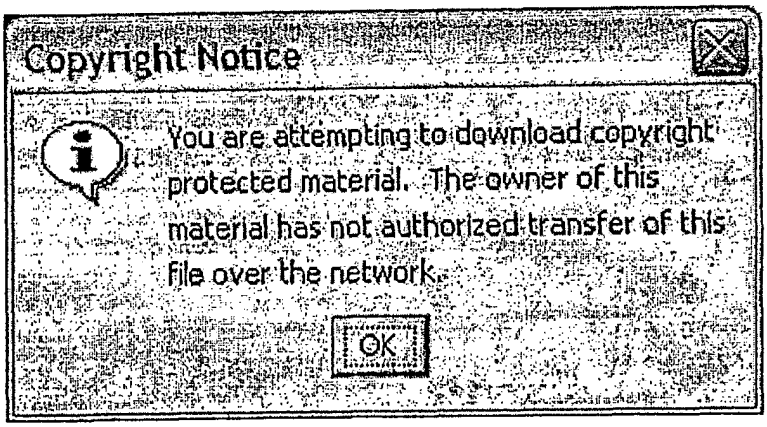

Copyright Notice
You are attempting to download copyright protected material. The owner of this material has not authorized transfer of this file over the network.
OK

Figure 4e

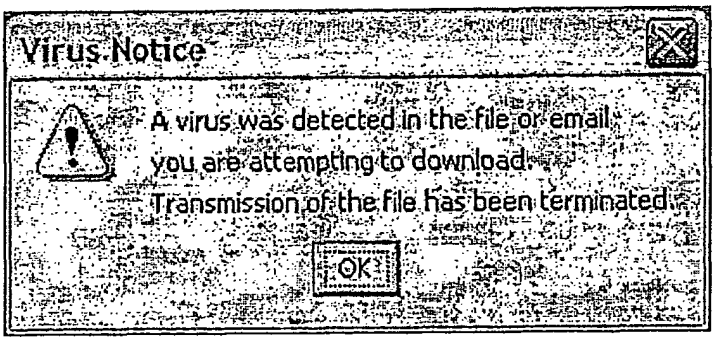


Figure 4f

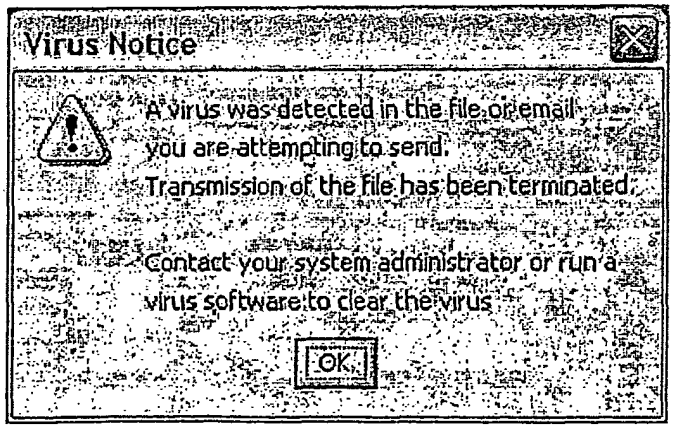


Figure 4g

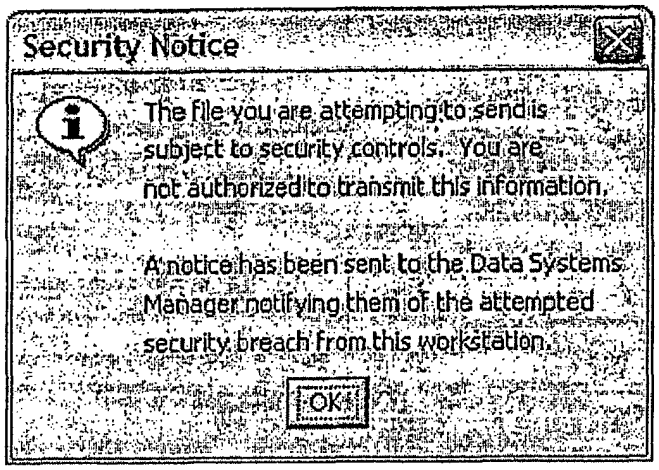


Figure 4h

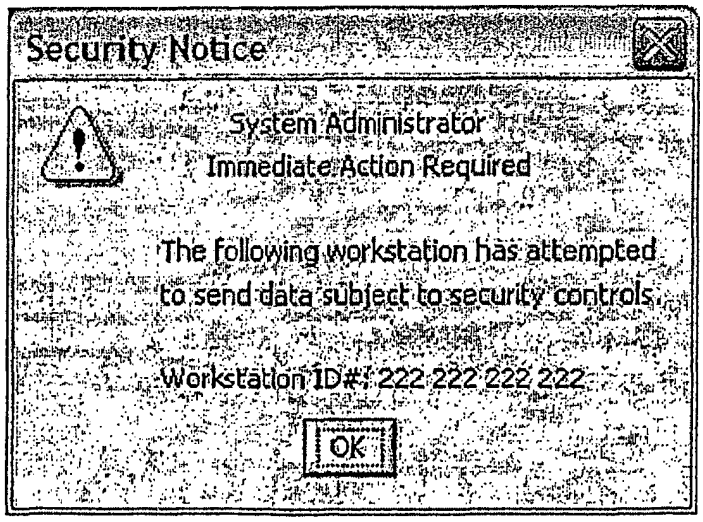
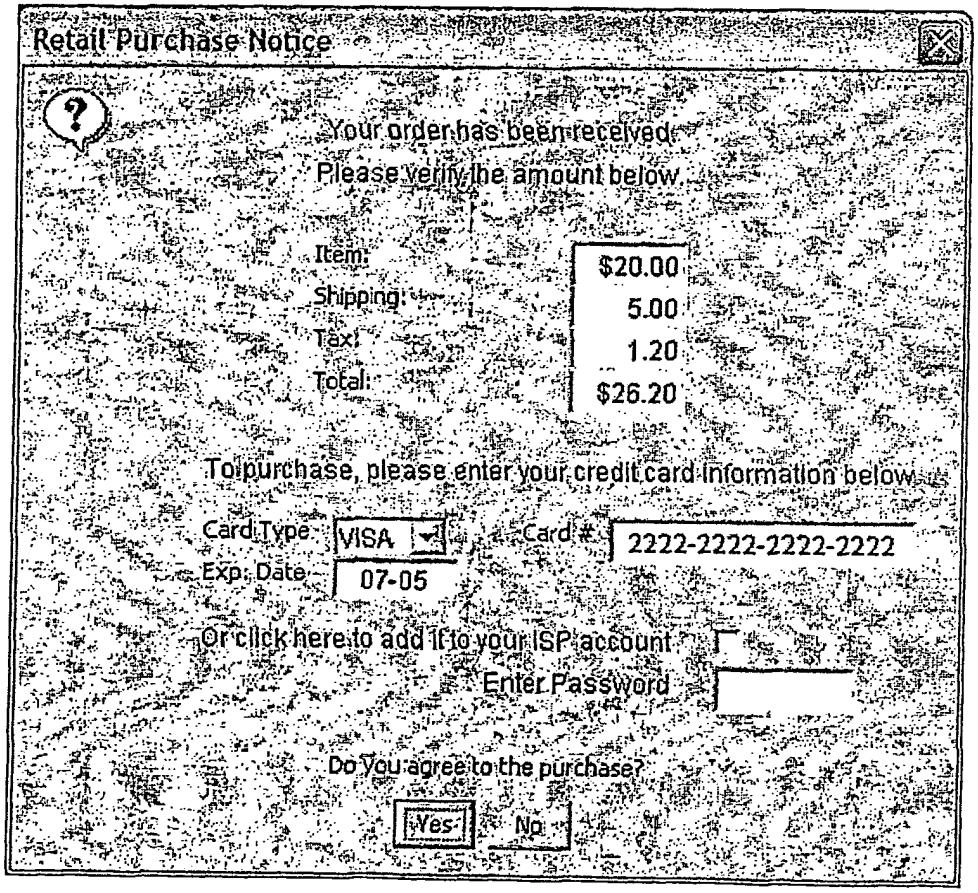


Figure 4i


Retail Purchase Notice
Your order has been received.
Please verify the amount below.
Item:
Shipping:
Tax:
Total:
$20.00
5.00
1.20
$26.20
To purchase, please enter your credit card information below.
Card Type:
VISA
Card #:
2222-2222-2222-2222
Exp. Date:
07-05
Or click here to add it to your ISP account
Enter Password
Do You agree to the purchase?
Yes
No

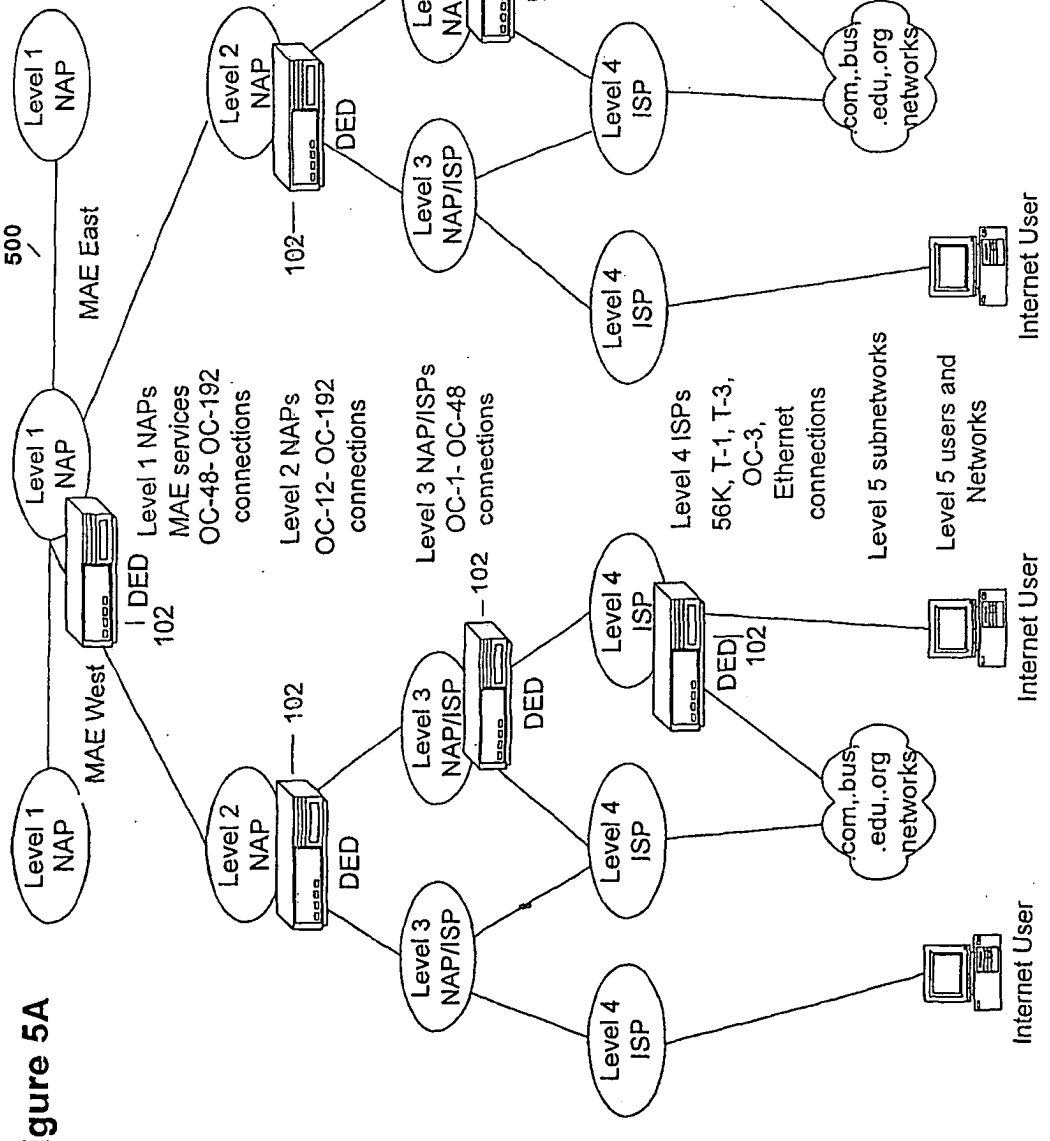

500
Level 1 NAP
MAE East
Level 1 NAP
MAE West
Level 1 NAPs MAE services OC-48- OC-192 connections
DED 102
Level 2 NAPs OC-12- OC-192 connections
Level 2 NAP
DED
102
Level 3 NAP/ISPs OC-1- OC-48 connections
Level 3 NAP/ISP
DED
102
Level 4 ISPs 56K, T-1, T-3, OC-3, Ethernet connections
Level 4 ISP
Level 5 subnetworks
com,.bus .edu,.org networks
Level 5 users and Networks
Internet User

Figure 5A

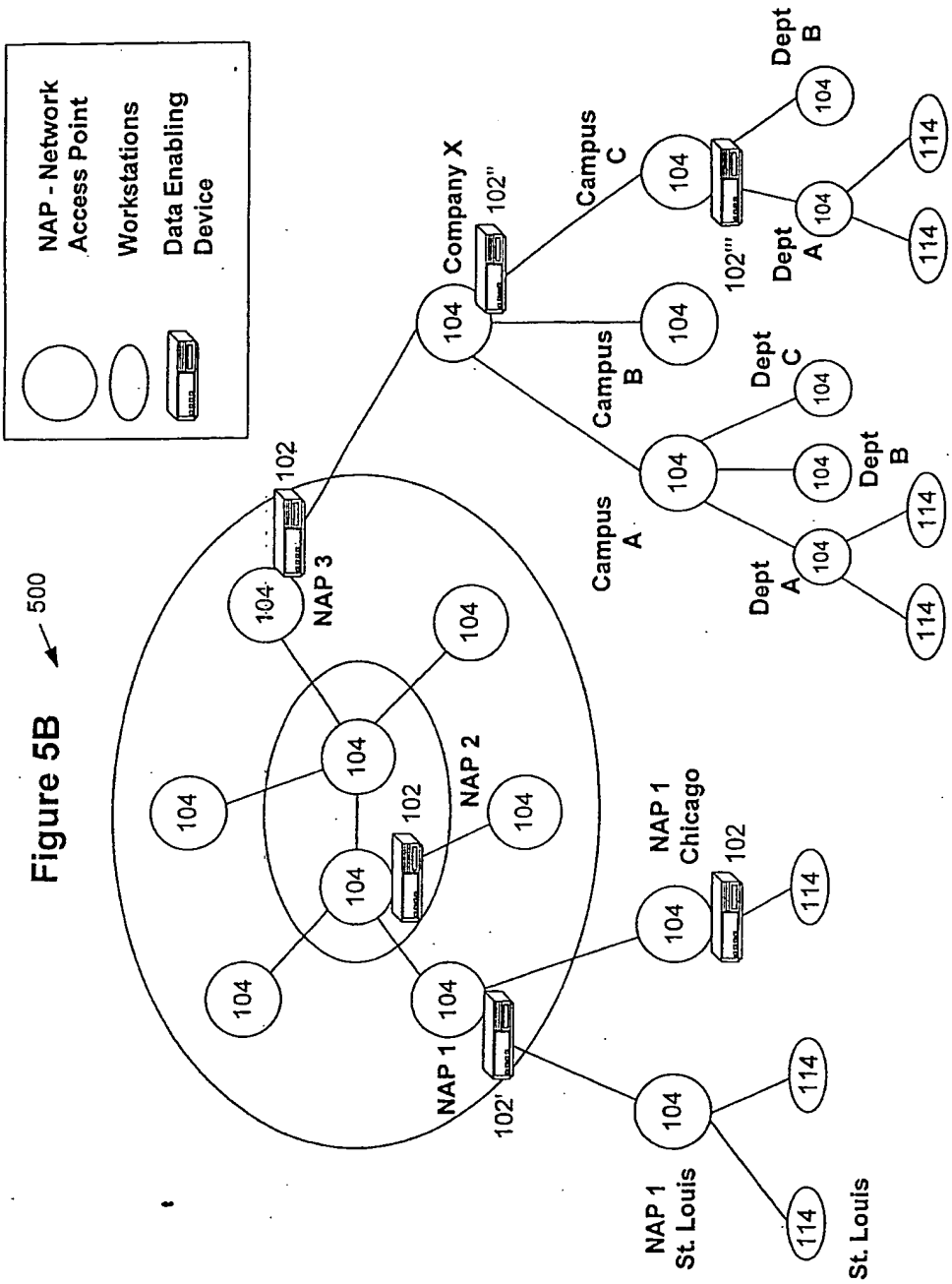

NAP - Network Access Point
Workstations
Data Enabling Device
500
NAP 3
NAP 2
NAP 1
102
102'
102''
102'''
Company X
Campus A
Campus B
Campus C
Dept A
Dept B
Dept C
NAP 1 Chicago
NAP 1 St. Louis
St. Louis
104
114

Figure 5B

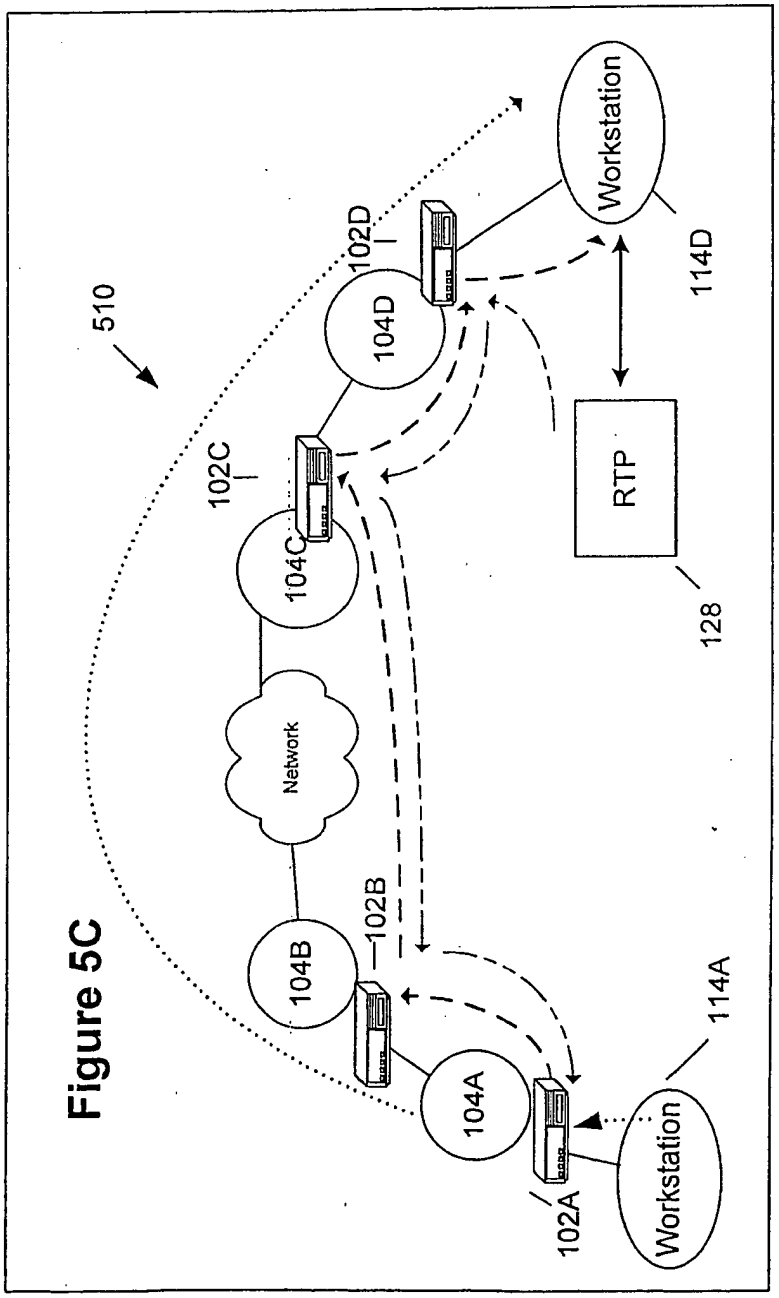

510
102A
102B
102C
102D
104A
104B
104C
104D
Network
RTP
128
Workstation
114A
Workstation
114D
Identified Content
Message
Release_Content
or
Cease_Content

Figure 5C

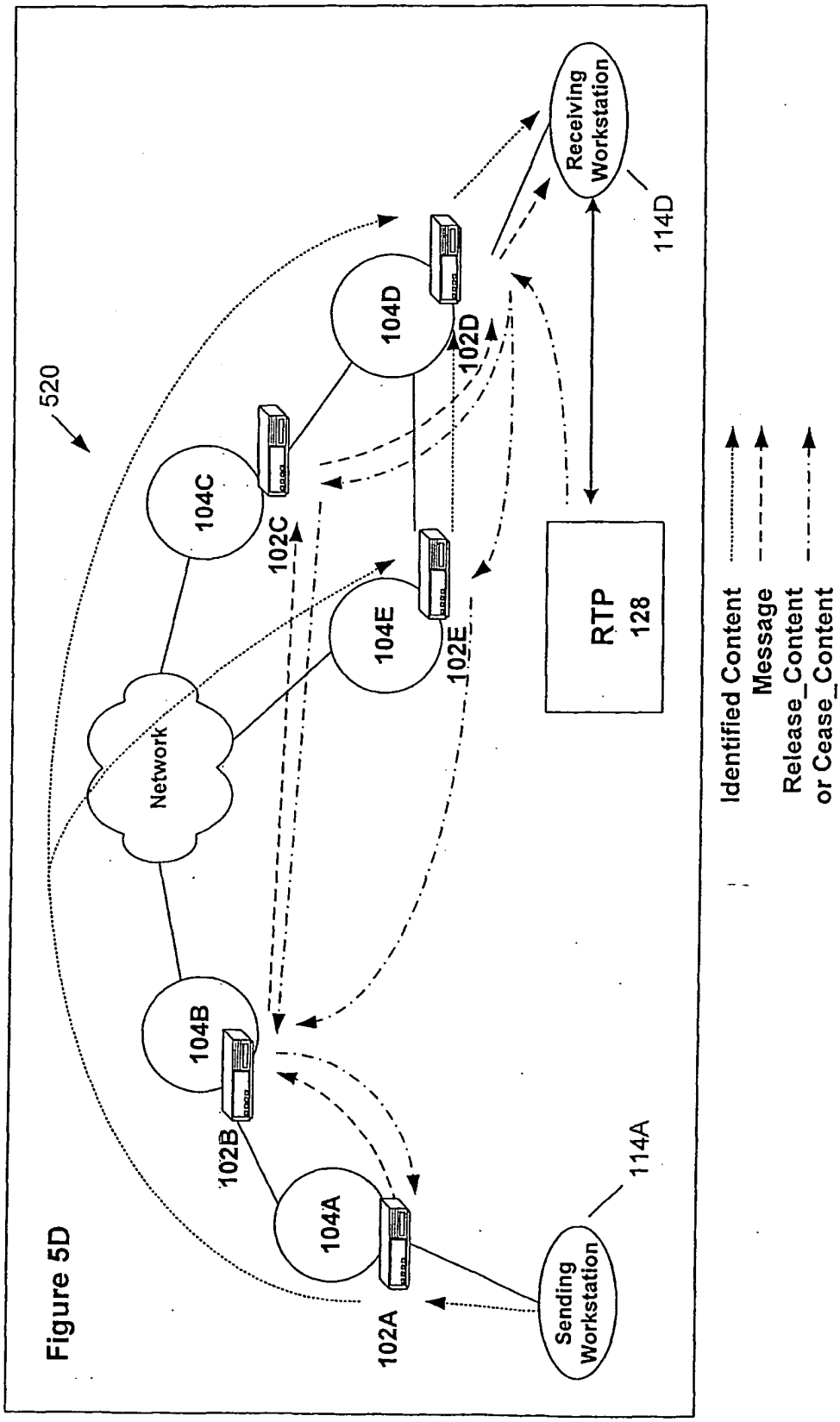

520
Receiving Workstation
114D
104D
102D
104C
102C
104E
102E
RTP
128
Network
104B
102B
104A
102A
Sending Workstation
114A
Identified Content
Message
Release_Content
or Cease_Content

Figure 5D

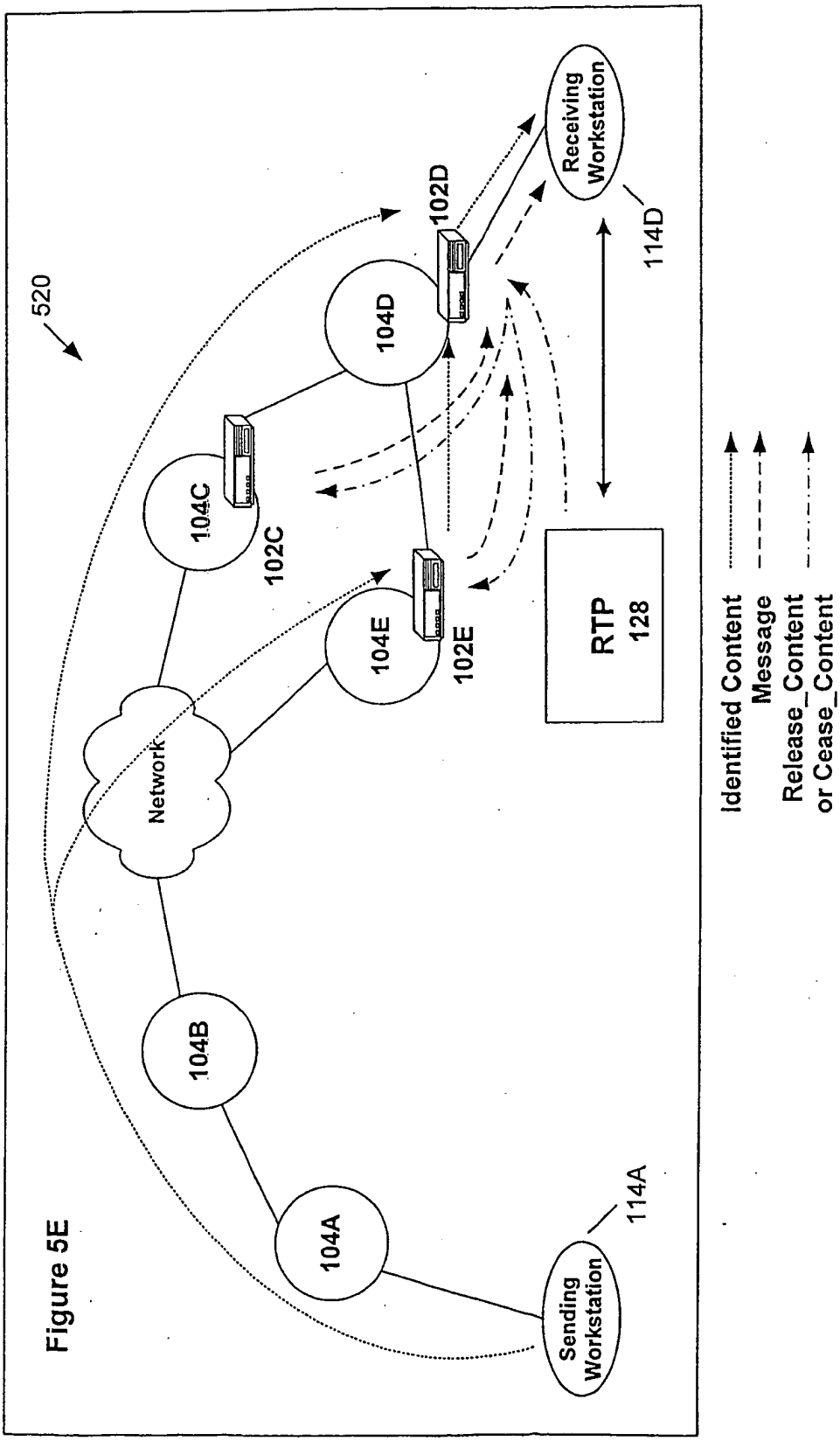

520
Receiving Workstation
114D
102D
104D
104C
102C
104E
102E
RTP
128
Network
104B
104A
Sending Workstation
114A
Identified Content
Message
Release_Content
or Cease_Content

Figure 5E

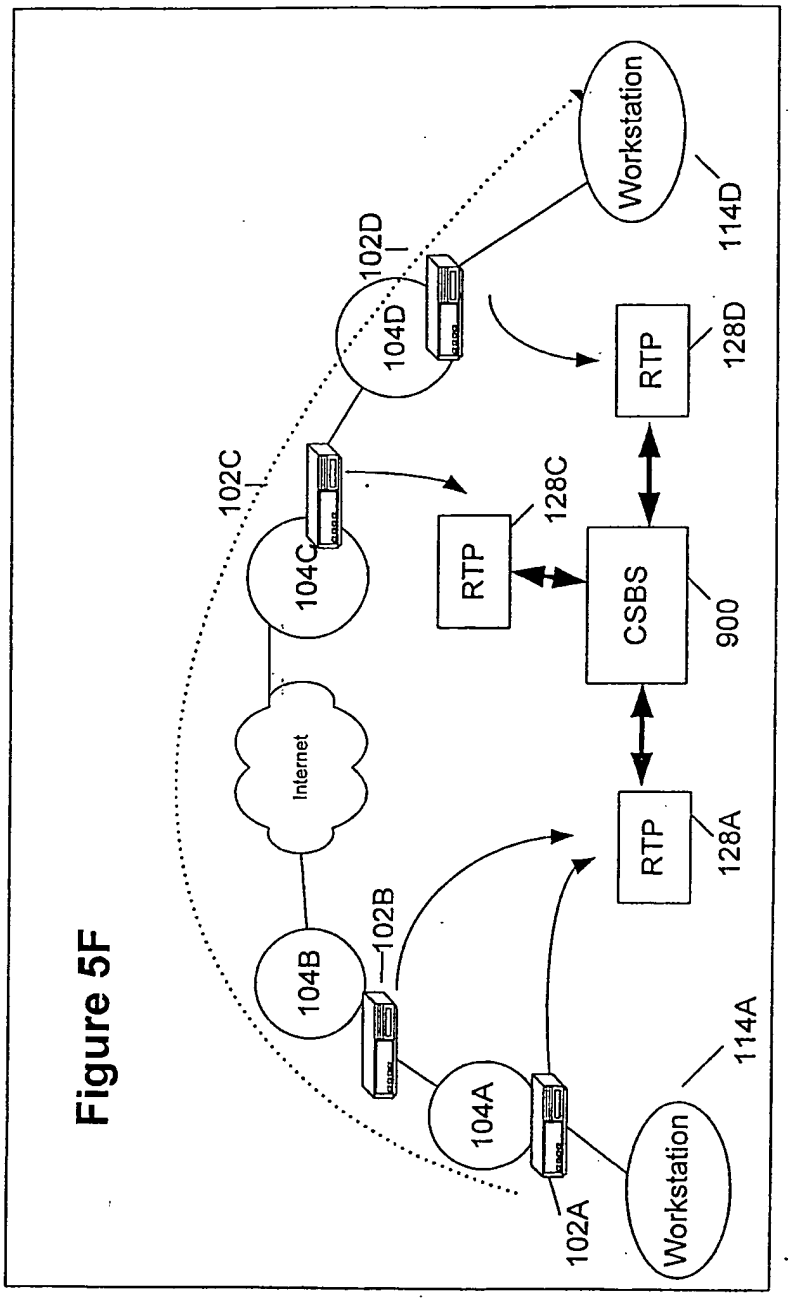
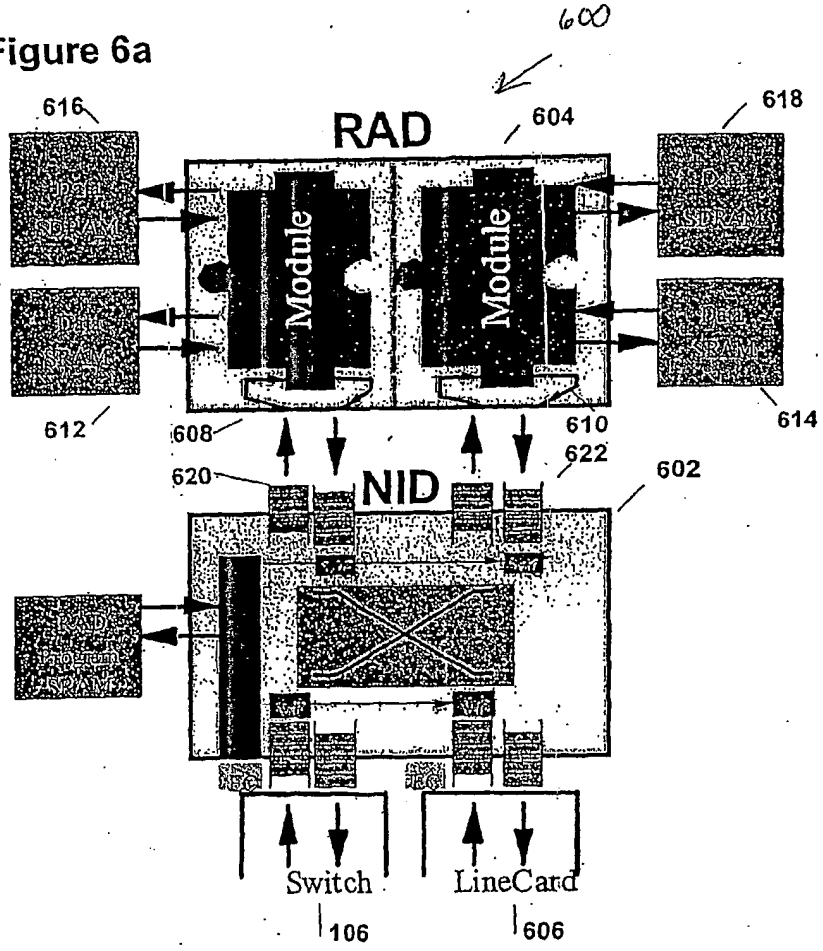


Figure 5F
Workstation
114D
102D
104D
RTP
128D
102C
104C
RTP
128C
CSBS
900
Internet
104B
102B
RTP
128A
104A
102A
Workstation
114A
Identified Content
Database Update

Figure 6a


600
RAD
604
616
618
Module
Module
612
608
610
614
620
NID
622
602
Switch
106
LineCard
606

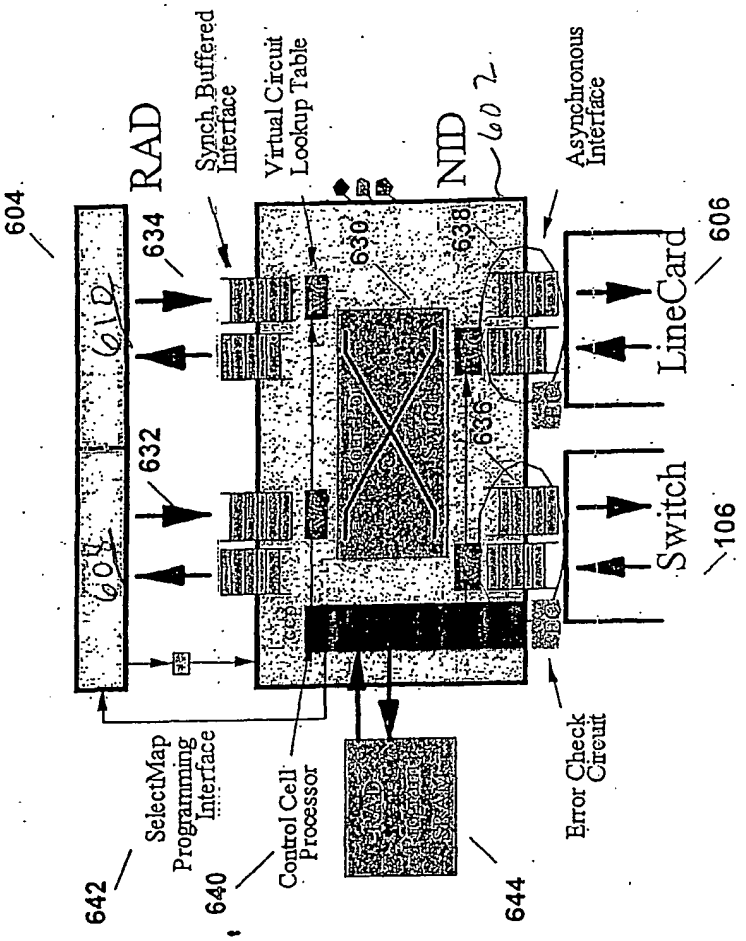

604
RAD
634
Synch Buffered Interface
Virtual Circuit Lookup Table
630
NID
602
638
Asynchronous Interface
606
LineCard
632
636
Switch
106
642
SelectMap Programming Interface
640
Control Cell Processor
644
Error Check Circuit

Figure 6b

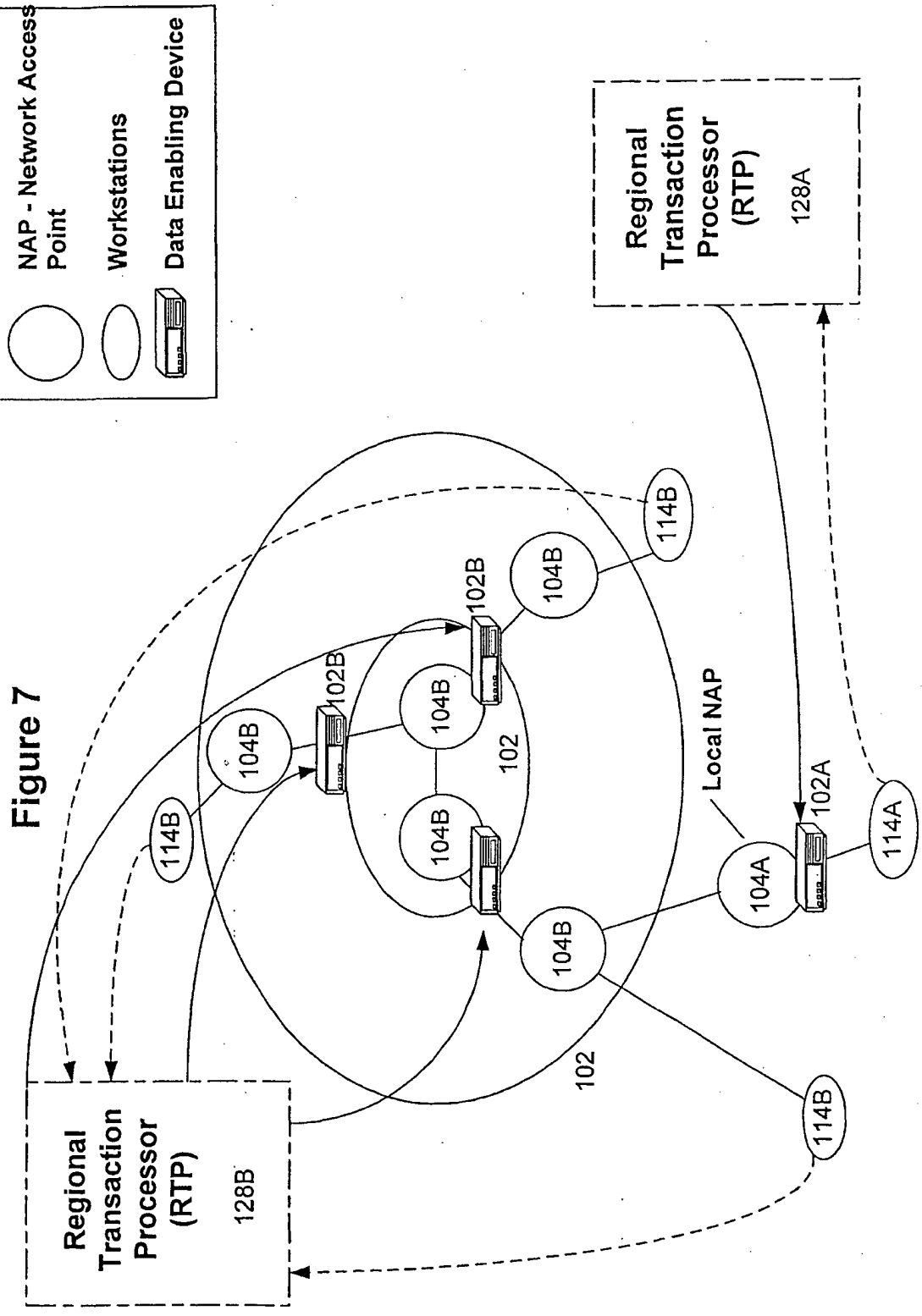

NAP - Network Access Point
Workstations
Data Enabling Device
Regional Transaction Processor (RTP)
128A
Regional Transaction Processor (RTP)
128B
Local NAP
102
102A
102B
104A
104B
114A
114B

Figure 7

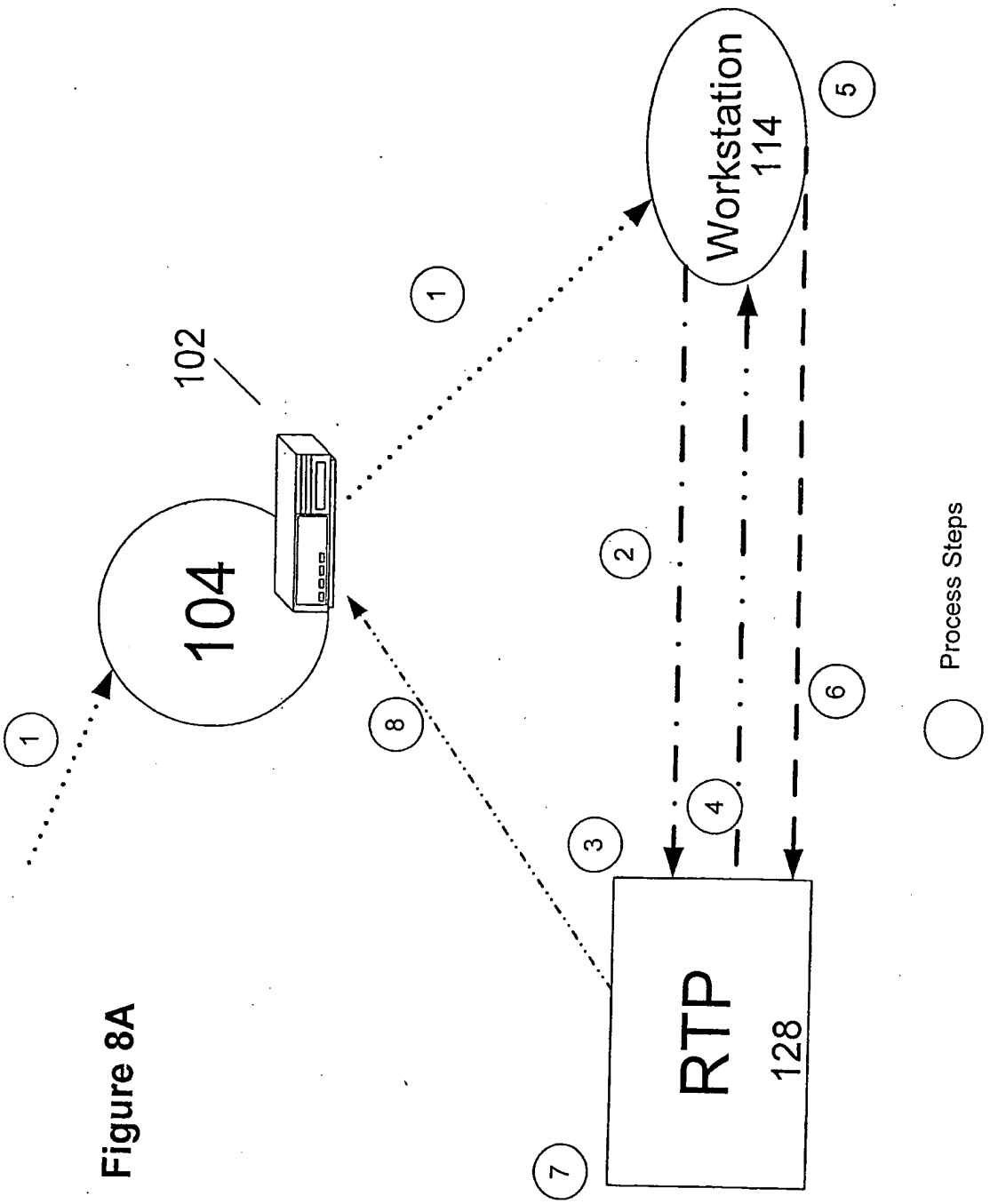


Figure 8A

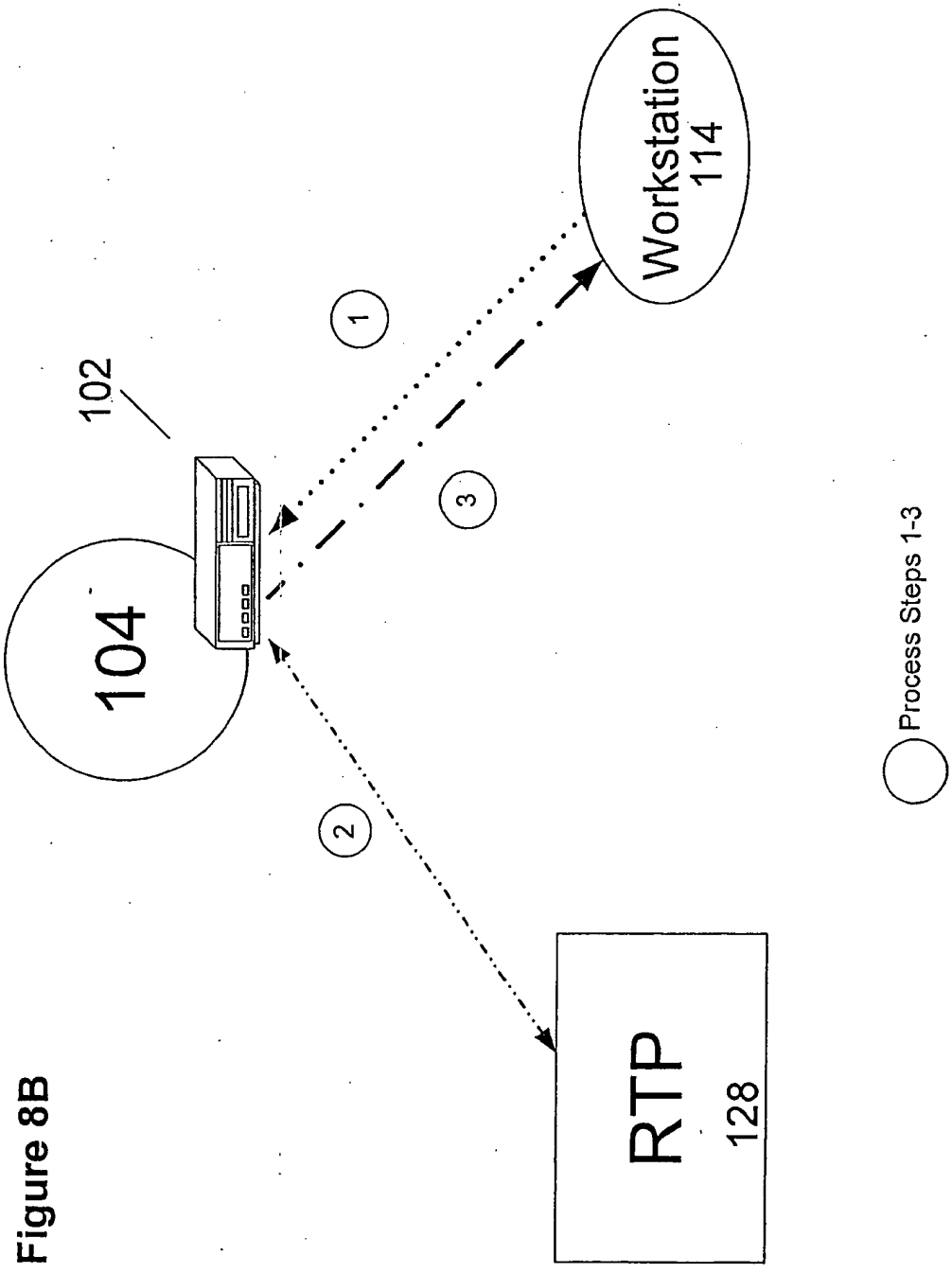


Figure 8B

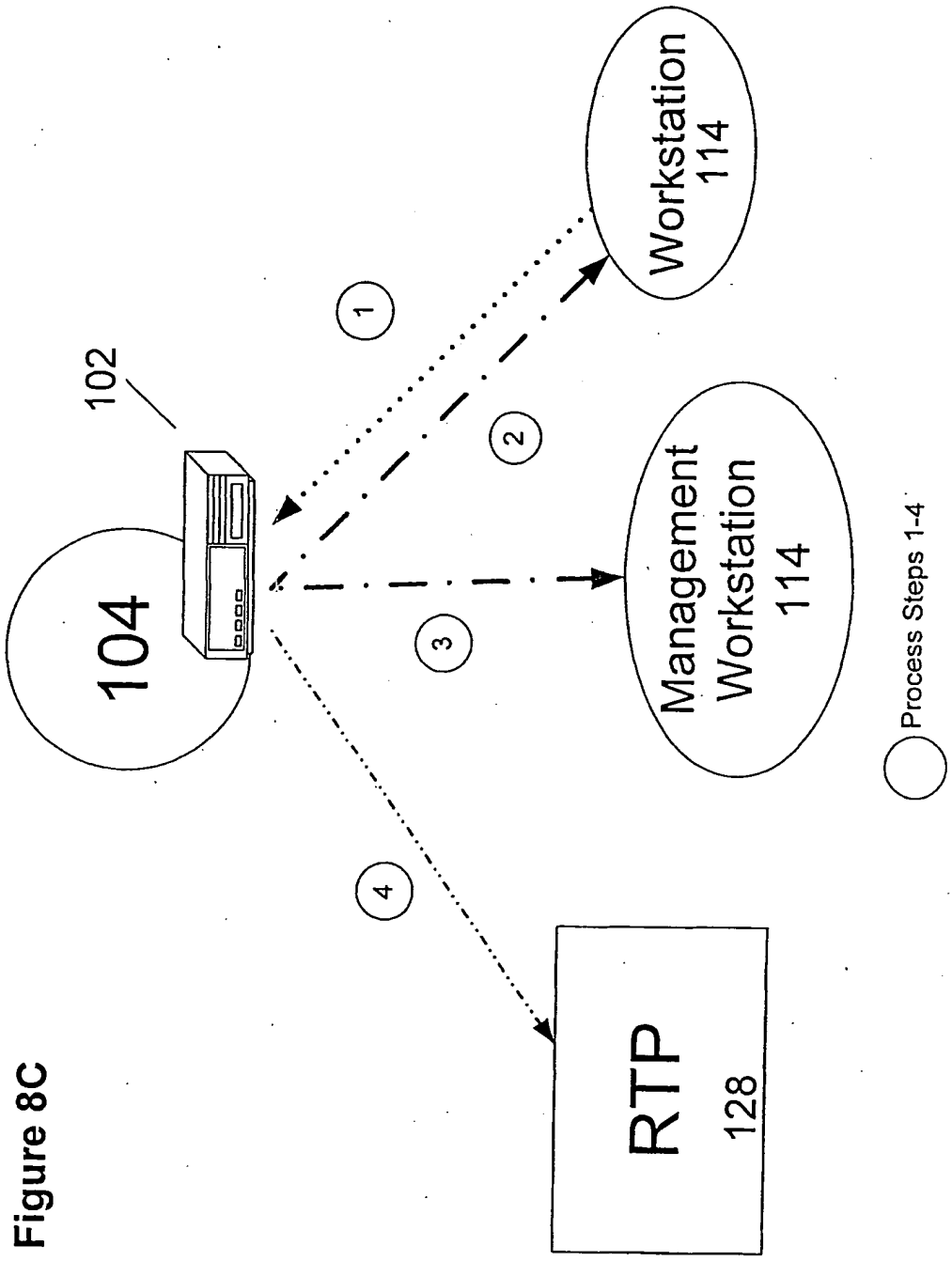

Workstation
114
102
104
1
2
3
4
Management
Workstation
114
RTP
128
Process Steps 1-4

Figure 8C

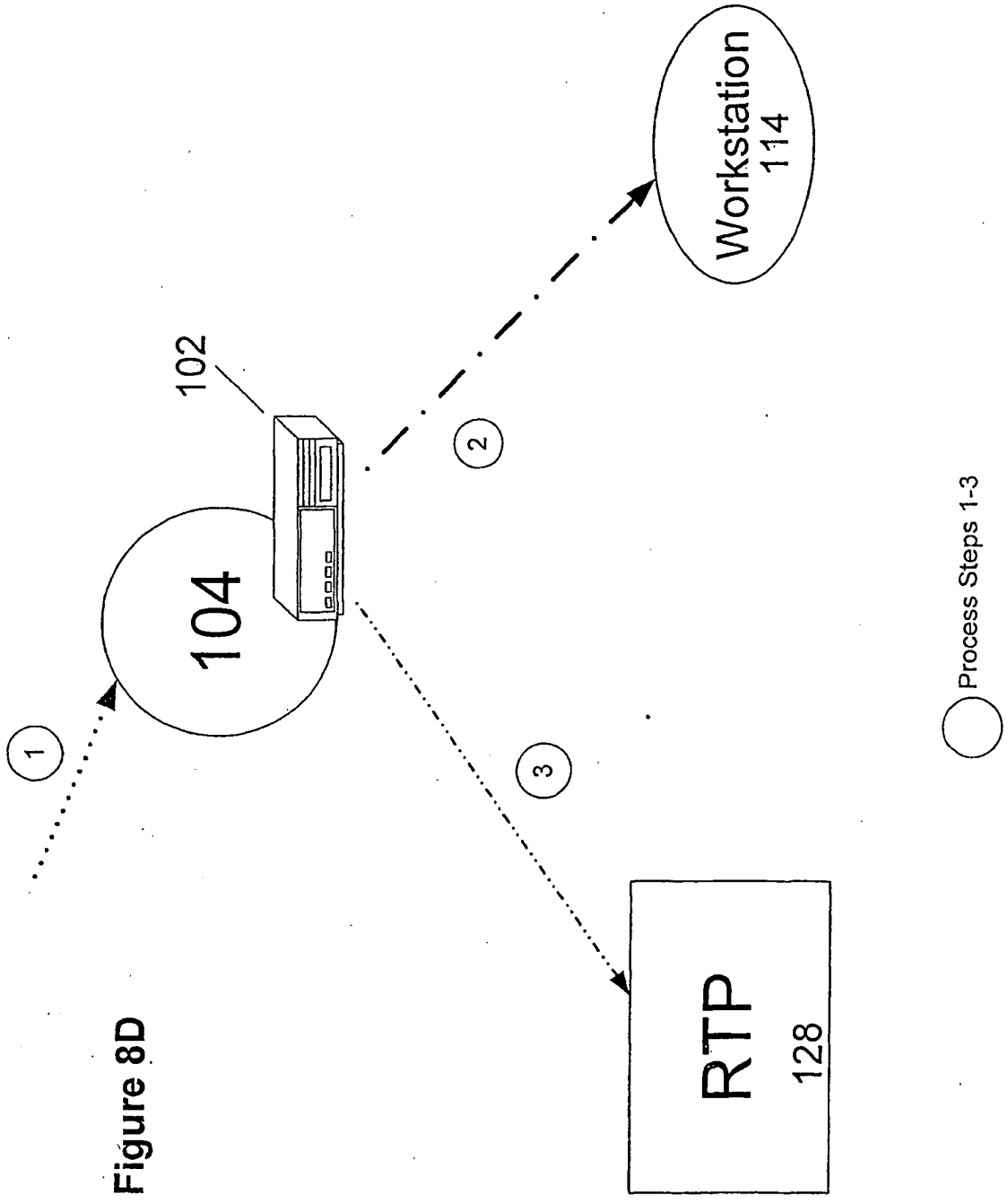


Figure 8D

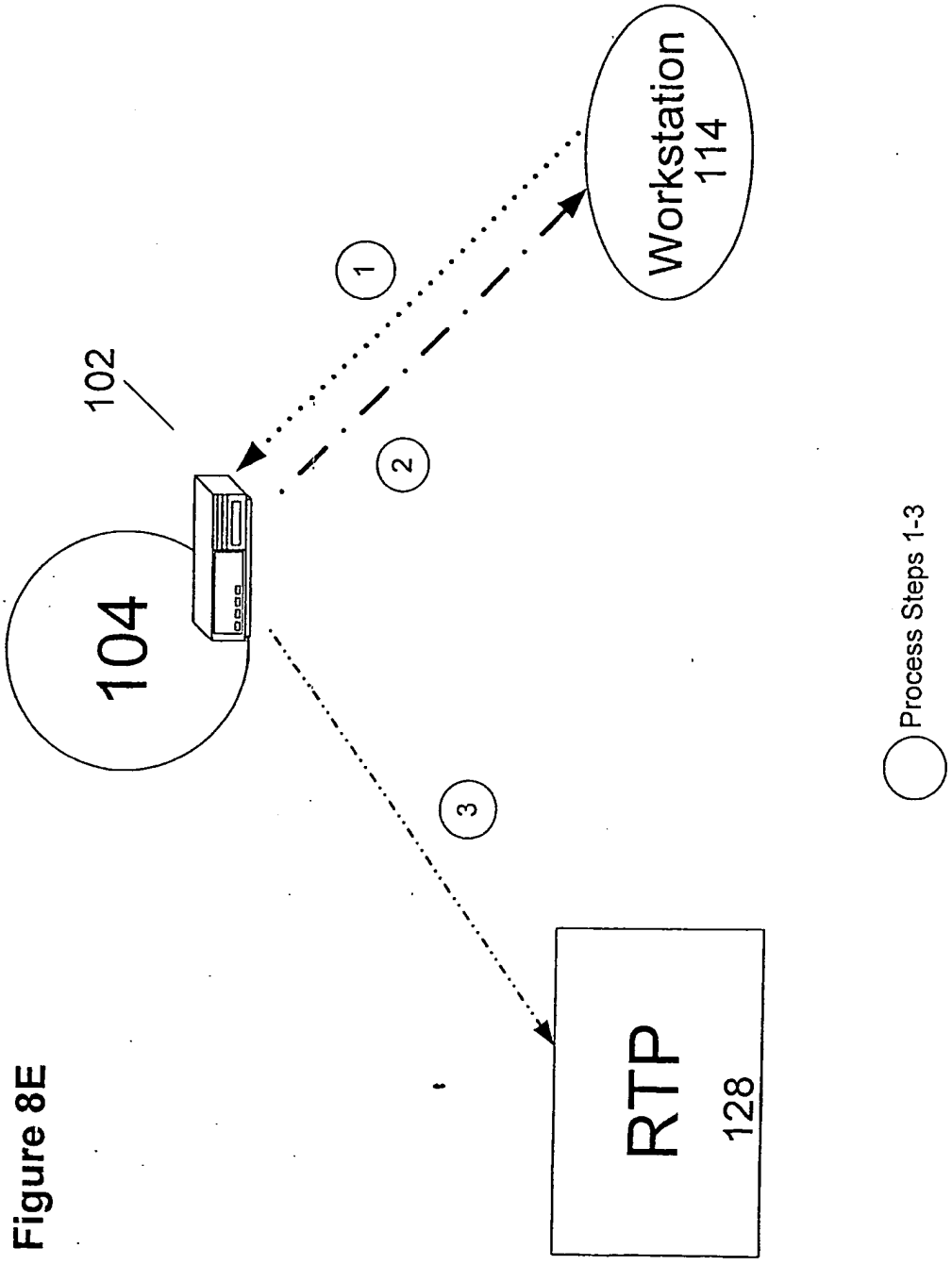
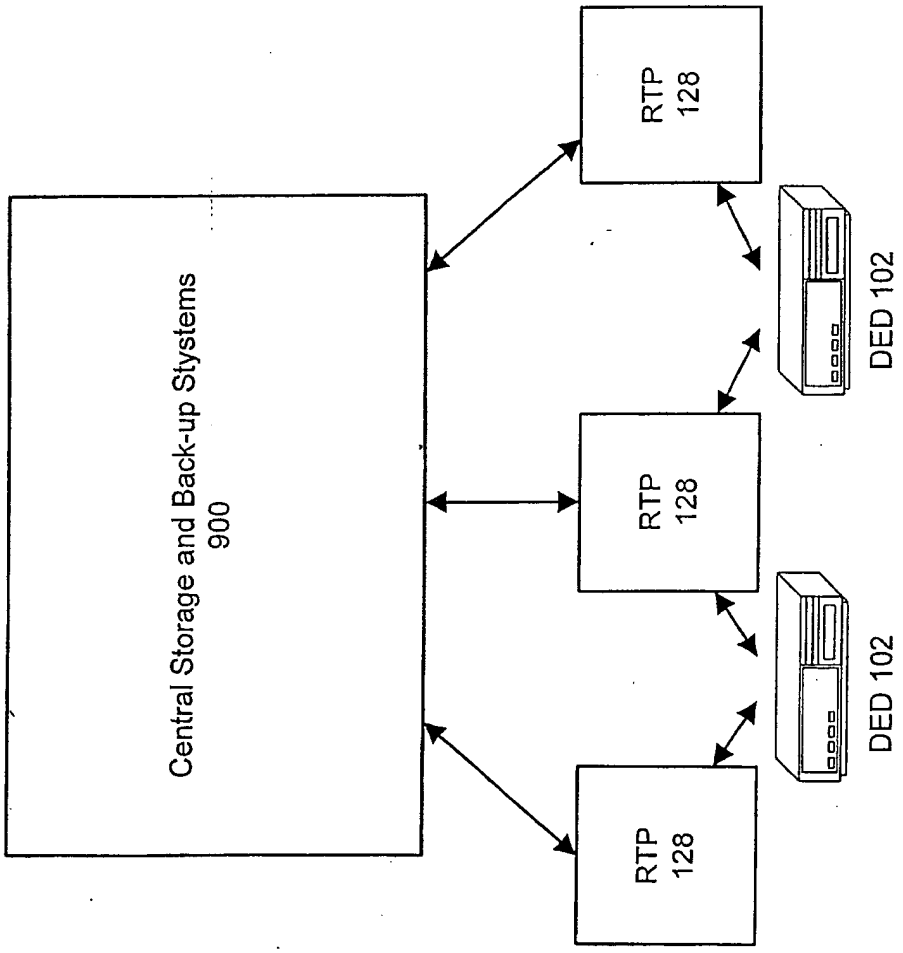


Figure 8E

Figure 9


Central Storage and Back-up Stystems
900
RTP
128
RTP
128
RTP
128
DED 102
DED 102

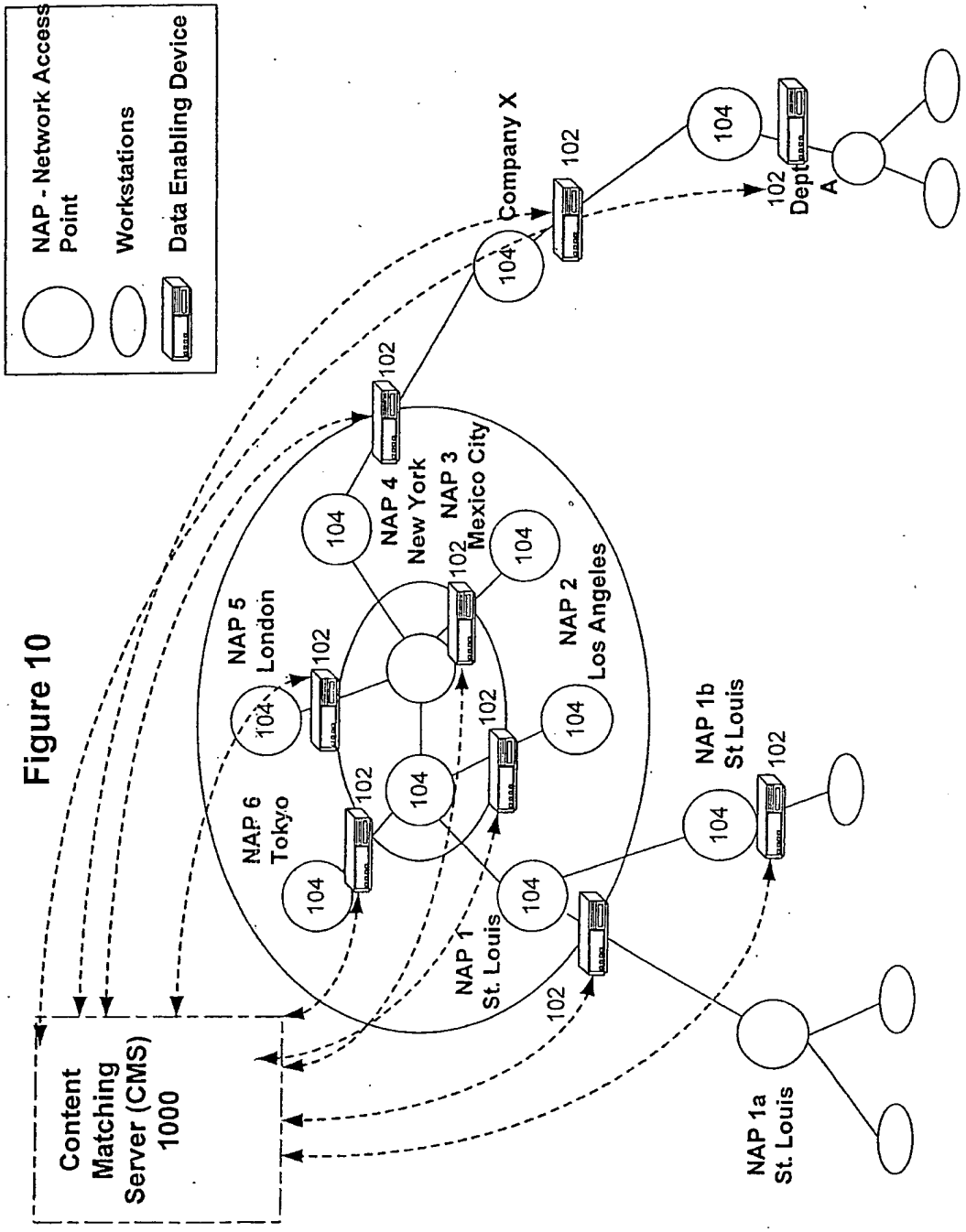

NAP - Network Access Point
Workstations
Data Enabling Device
Content Matching Server (CMS) 1000
NAP 1 St. Louis
NAP 1a St. Louis
NAP 1b St Louis
NAP 2 Los Angeles
NAP 3 Mexico City
NAP 4 New York
NAP 5 London
NAP 6 Tokyo
Company X
Dept A
102
104

Figure 10

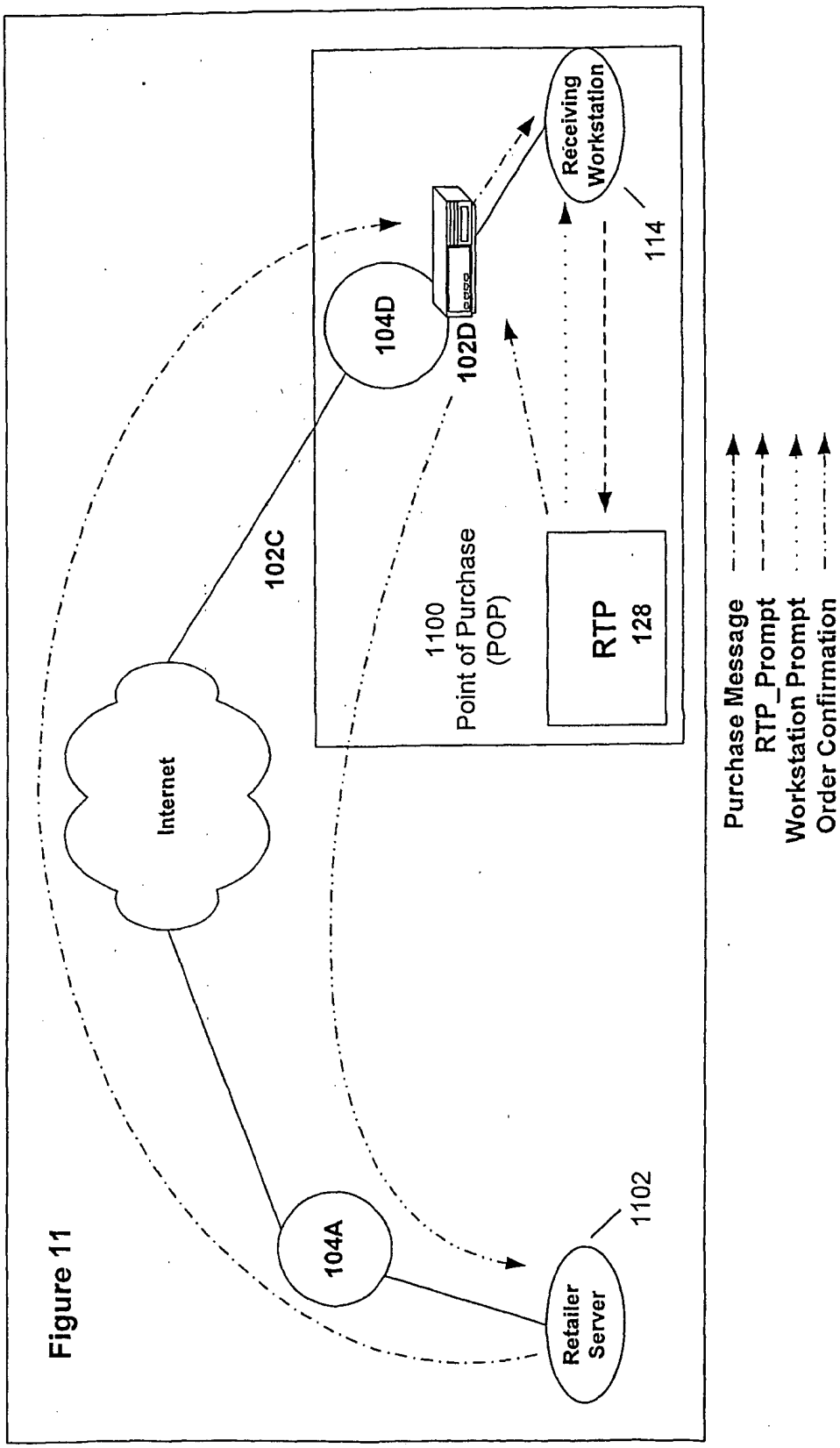

Receiving Workstation
114
104D
102D
102C
1100
Point of Purchase
(POP)
RTP
128
Internet
104A
Retailer Server
1102
Purchase Message
RTP_Prompt
Workstation Prompt
Order Confirmation

Figure 11

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 May 2003 (01.05.2003)

PCT

(10) International Publication Number
WO 03/036845 A3

(51) International Patent Classification[7]: G06F 15/173

(21) International Application Number: PCT/US02/33286

(22) International Filing Date: 18 October 2002 (18.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/037,593 19 October 2001 (19.10.2001) US

(71) Applicant *(for all designated States except US)*: **GLOBAL VELOCITY, L.L.C.** [US/US]; 211 N. Broadway, Suite 2200, St. Louis, MO 63102 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KULIG, Matthew, P.** [—/—]; 19 Danube Dr., Millstadt, IL 62260 (US). **BROOKS, Timmy, L.** [—/—]; 1836 Meadow Trails Dr., St. Louis, MO 63130 (US). **LOCKWOOD, John, W.** [—/—]; 839 Jackson Ave., St. Louis, MO 63130 (US). **REDDICK, David, Kyle** [—/—]; 512 S. Clay Ave., Kirkwood, MO 63122 (US).

(74) Agents: **BERTANI, Mary Jo** et al.; Koestner Bertani LLP, 18662 MacArthur Blvd., Suite 400, Irvine, CA 92612 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

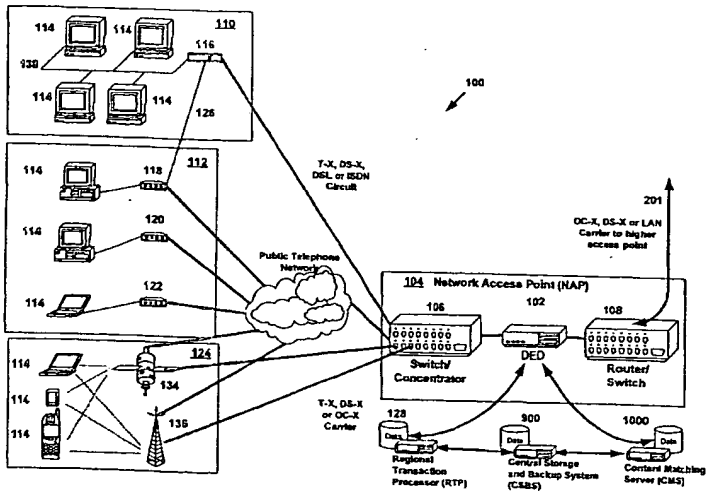
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
16 October 2003

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR CONTROLLING TRANSMISSION OF DATA PACKETS OVER AN INFORMATION NETWORK



(57) Abstract: An apparatus for controlling transmission of data packets in an information network comprises a Regional Transaction Processor (128) (RTP) operable to communicate with a Data Enabling Device (DED) and at least one workstation. The DED (102) searches data packets for content match information. The RTP (128) includes instructions to generate information to include in a prompt to be presented at the workstation when the content match information is detected in at least one of the data packets. The prompt is based on information in the data packet. Transmission of the data packets through the information network is suspended by the DED (102) until a response to the prompt is received that authorizes downloading the data packets to the workstation. If transmission of the data packets to the workstation is not authorized, the data packets are discarded by the DED.

WO 03/036845 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/33286

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : GO6F 15/173
US CL : 709/225
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/225

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST. GOOGLE.COM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 2002/0116508 A1 (KHAN et al) 22 August 2002 (22.08.2002), See abstract , paragrtaphs [0052] - [0054]	1-53
A	US 6,259,909 B1 (RATAYCZAK ET AL) 10 July 2001 (10.07.2001),abtract, col. 5, lines 30-54	1, 18, 28, 36, and 49
A	U.S. 5,761,431 A (GROSS et al) 02 June 1998 (02.06.1998) col.6, lines 1-7	1, 18, 28, 36, and 49
A,P	US 6,343,324 B1 (HUBIS et al) 29 January 2002 (29.01.2002), See Abstract	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 2002 (16.12.2002)	22 JAN 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Glen Burgess Peggy Harrod Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)